

Sygn. akt: KIO 2024/19

WYROK
z dnia 28 października 2019 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Ewa Kisiel

Protokolant: Adam Skowroński

po rozpoznaniu na rozprawie w dniu 22 października 2019 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 10 października 2019 r. przez wykonawcę **MIRBUD S.A. z siedzibą w Skierniewicach przy ul. Unii Europejskiej 18** w postępowaniu prowadzonym przez zamawiającego **Komendę Wojewódzką Policji w Poznaniu przy ul. Jana Kochanowskiego 2A;**

przy udziale wykonawcy **Alstal Grupa Budowlana sp. z o.o. sp. k. z siedzibą w Jacewie przy ul. Kwiatowej 23** zgłaszającego przystąpienie do postępowania odwoławczego po stronie zamawiającego

orzeka:

1. **oddala odwołanie;**
2. kosztami postępowania obciąża wykonawcę **MIRBUD S.A. z siedzibą w Skierniewicach przy ul. Unii Europejskiej 18** i:
 - 2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **20 000 zł 00 gr** (słownie: dwadzieścia tysięcy złotych zero groszy) uiszczoną przez wykonawcę **MIRBUD S.A. z siedzibą w Skierniewicach przy ul. Unii Europejskiej 18** tytułem wpisu od odwołania,

- 2.2.** zasądza od wykonawcy **MIRBUD S.A. z siedzibą w Skierniewicach przy ul. Unii Europejskiej 18** na rzecz zamawiającego **Komendy Wojewódzkiej Policji w Poznaniu przy ul. Jana Kochanowskiego 2A** kwotę **3 600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy), stanowiącą koszty postępowania odwoławczego poniesione z tytułu wynagrodzenia pełnomocnika.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 ze zm.) na niniejszy wyrok – w terminie 7 dni od dnia jego doręczenia przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Poznaniu.

Przewodniczący:

UZASADNIENIE

Komenda Wojewódzka Policji w Poznaniu przy ul. Jana Kochanowskiego 2A (dalej: „Zamawiający”), na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018 r., poz. 1986 j.t. ze zm.) - zwanej dalej "ustawą" lub "Pzp" – prowadzi w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia na pn. „Budowa nowej siedziby Komendy Powiatowej Policji w Pile”, numer sprawy ZZP-2380-46/2019.

Szacunkowa wartość przedmiotowego zamówienia jest wyższa od kwot wskazanych w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 Pzp.

Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej z dnia 17 lipca 2019 r. pod nr 2019/S 136-334314. Zamawiający zamieścił specyfikację istotnych warunków zamówienia (dalej: „SIWZ" lub „specyfikacja”) na stronie internetowej pod adresem: <http://bip.poznan.kwp.policia.Rov.pl/KWP/zamowienia-publiczne/ogloszenia-o-wszczeciu/>

W dniu 30 września 2019 r., drogą elektroniczną, Zamawiający poinformował wykonawcę MIRBUD S.A. z siedzibą w Skierniewicach przy ul. Unii Europejskiej 18 (dalej: „Odwołujący” lub „Mirbud”) o tym, że odrzucił ofertę Odwołującego na podstawie art. 89 ust. 1 pkt 2 Pzp.

W dniu 10 października 2019 r. wykonawca Mirbud wniósł do Prezesa Krajowej Izby Odwoławczej odwołanie od niezgodnych z przepisami ustawy czynności Zamawiającego podjętych oraz zaniechanych w postępowaniu, tj. od:

- a) czynności badania i oceny oferty złożonej przez Odwołującego,
- b) czynności odrzucenia oferty Odwołującego na podstawie art. 89 ust. 1 pkt 2 Pzp,
- c) zaniechania czynności poprawienia w ofercie Odwołującego innej omyłki, polegającej na niezgodności oferty ze specyfikacją, niepowodującej istotnych zmian w treści oferty,

- d) zaniechania przedstawiania rzeczowej argumentacji i wskazania okoliczności faktycznych uzasadniających odrzucenie oferty Odwołującego,
- e) z ostrożności procesowej - od zaniechania wezwania Odwołującego do wyjaśnień treści oferty co doprowadziło do jej bezprawnego odrzucenia.

Wykonawca Mirbud w treści odwołania postawił zarzuty naruszenia przez Zamawiającego:

1. art. 7 ust. 1 Pzp w związku z naruszeniem art. 89 ust. 1 pkt 2 Pzp przez odrzucenie oferty Odwołującego, pomimo że jej treść odpowiada treści SIWZ;
2. art. 7 ust. 1 Pzp w związku z naruszeniem art. 87 ust. 2 pkt 3 Pzp przez zaniechanie poprawienia w ofercie Odwołującego innej omyłki polegającej na niezgodności oferty z SIWZ, niepowodującej istotnych zmian w treści oferty i w konsekwencji naruszenie art. 89 ust. 1 pkt 2 Pzp przez odrzucenie oferty Odwołującego;
3. art. 7 ust. 1 Pzp w związku z naruszeniem art. 92 ust. 1 pkt 3 Pzp przez przedstawianie uzasadnienia faktycznego odrzucenia oferty Odwołującego w sposób lakoniczny, pozbawiony rzeczowej argumentacji i bez wskazania okoliczności faktycznych uzasadniających odrzucenie oferty Odwołującego;
4. z ostrożności procesowej - zarzut naruszenia art. 7 ust. 1 Pzp w związku z art. 87 ust. 1 Pzp przez zaniechanie wezwania Odwołującego do wyjaśnień treści oferty co doprowadziło do jej bezprawnego odrzucenia, pomimo że w toku badania ofert Zamawiający jest zobowiązany do wyjaśniania wszelkich wątpliwości, a w szczególności tych, które skutkują uznaniem oferty Odwołującego za podlegającą odrzuceniu.

Odwołujący wnosił o uwzględnienie odwołania i nakazanie Zamawiającemu, aby:

- unieważnił czynność odrzucenia oferty Odwołującego;
- powtórzył czynność badania i oceny oferty Odwołującego, w tym w razie konieczności wezwał Odwołującego do złożenia wyjaśnień treści oferty na podstawie 87 ust. 1 Pzp;
- poprawił w ofercie Odwołującego inną omyłkę polegającą na niezgodności oferty z SIWZ, niepowodującą istotnych zmian w treści oferty, w sposób wskazany w treści odwołania;
- w konsekwencji dokonał wyboru oferty Odwołującego jako najkorzystniejszej oferty.

W uzasadnieniu odwołania wykonawca Mirbud wyjaśniał, że:

Ad I.

Punkt 1.1 Informacji o odrzuceniu ofert.

Wykonawca Mirbud, w zakresie zaoferowanego przez niego systemu kontroli dostępu firmy UTC Fire&Securite Sp. z o.o. (dalej: „firmy UTC”) podnosił, że nigdzie w SIWZ Zamawiający nie zakazał, ani pośrednio, ani wprost, wykorzystania central ATS do budowy systemu, w szczególności zakaz taki nie wynika z przytoczonego przez Zamawiającego fragmentu dokumentacji wykonawczej. Zamawiający wskazał tam jedynie, że system kontroli dostępu ma być zbudowany w oparciu o sterowniki sieciowe wraz z kontrolerami sieciowymi i serwerem dedykowanym do kontroli dostępu - i tak też będzie zbudowany system zaoferowany przez Odwołującego. Ani z oferty Odwołującego, ani ze złożonych przez niego wyjaśnień nie wynika nic innego. Jedyna różnica pomiędzy SIWZ a systemem zaoferowanym przez Odwołującego dotyczy nazewnictwa: to, co w dokumentacji wykonawczej jest określone mianem sterowników sieciowych, producent zaoferowanego systemu kontroli dostępu, czyli firma UTC określa mianem central ATS. Na tym jednak różnice się kończą. Odwołujący podnosił, że niezgodne z prawdą jest stwierdzenie Zamawiającego jakoby Odwołujący wskazał, że centrale ATS będą również pełnić funkcje central alarmowych, co w rezultacie ma spowodować zmniejszenie niezawodności systemu. W rzeczywistości nic takiego nie wynika ani z oferty Odwołującego, ani ze złożonych przez niego wyjaśnień. Odwołujący wskazywał, że centrale ATS (sterowniki sieciowe wg nazewnictwa dokumentacji projektowej) nie będą pełniły funkcji central alarmowych, lecz będą wyłącznie sterownikami sieciowymi. Zamawiający powinien mieć zresztą tego świadomość, gdyż jak słusznie zauważył w pkt 1.1. Informacji o odrzuceniu ofert Odwołujący w formularzu ofertowym wykazał, że systemy alarmowe (w tym system sygnalizacji włamania i napadu, w skrócie: SSWiN, zamierza wykonać przy wykorzystaniu rozwiązań innych producentów niż firmy UTC. Odwołujący jako SSWiN zaoferował system producenta SATEL sp. z o.o., czyli inny system innego producenta.

Odnosnie central ATS Zamawiający zarzucił ponadto Odwołującemu w pkt 1.1., że: „Również awaria central spowoduje wyłączenie obu systemów, co jest dla Zamawiającego niedopuszczalne.” Odwołujący stwierdził, że powyższe stwierdzenie jest niezgodne z prawdą z powodów opisanych powyżej. Tym samym awaria central ATS nie spowoduje wyłączenia obu systemów. Odwołujący wskazywał i podkreślał, że na poziomie sprzętowym każda centrala ATS (sterownik sieciowy wg nazewnictwa dokumentacji projektowej) posiada własny monitorowany zasilacz buforowy, pełną bazę danych użytkowników i ich uprawnień oraz rejestr zdarzeń. Nie

ma zatem ani ryzyka nadpisywania zdarzeń, ani wyłączenia systemu kontroli dostępu wskutek utraty łączności z serwerem. Niezależność central ATS i każdego kontrolera sieciowego pozawala zachować funkcjonalność kontroli dostępu nawet w wypadku awarii centrali ATS czy utraty łączności pomiędzy kontrolerami czy serwerem na dłuższy czas.

Odnosnie kolejnych stwierdzeń Zamawiającego w zakresie zaoferowanego przez Odwołującego systemu kontroli dostępu firmy UTC podnosił on, że nigdzie w SIWZ Zamawiający nie zakazał, ani pośrednio, ani wprost, zaoferowania rozwiązania opartego o wykorzystanie fizycznego interfejsu RS485, a w szczególności zakaz taki nie wynika z przytoczonego przez Zamawiającego fragmentu dokumentacji wykonawczej. Odwołujący wyjaśniał, że Zamawiający narzucił konkretny rodzaj interfejsu tylko i wyłącznie w przypadku:

- komunikacji sterowników sieciowych i kontrolerów sieciowych, tj. interfejs CAN,
- komunikacji kontrolerów sieciowych i czytników kontroli dostępu, tj. jeden z dwóch protokołów (interfejsów): AbaTRACK II albo Wiegand.

Odwołujący twierdził, że powyższe wymagania co do interfejsów CAN i Wiegand zaoferowany przez Odwołującego system kontroli dostępu spełnia. Natomiast w pozostałym zakresie Zamawiający dał wykonawcom swobodę w doborze interfejsów. Tym samym wykorzystanie fizycznego interfejsu RS485 w zaoferowanym rozwiązaniu nie stanowi i nie może stanowić niezgodności treści oferty z treścią SIWZ. Niezależnie od powyższego Odwołujący wskazywał, że nie zgadza się z negatywną oceną Zamawiającego dotyczącą fizycznego interfejsu RS485. W ocenie Odwołującego interfejs ten nie jest przestarzały, przeciwnie, jest to rozwiązanie nowocześniejsze i daleko bardziej bezpiecznie od interfejsów CAN i Wiegand. Nieprawdziwe jest też twierdzenie Zamawiającego, że interfejs RS485 nie jest stosowany w nowoczesnych systemach kontroli dostępu, gdyż w rzeczywistości jest stosowany bardzo często. Nieprawdziwe jest też twierdzenie Zamawiającego, że wykorzystanie interfejsu RS485 spowoduje wolniejszą niż projektowana prace urządzeń w tak rozbudowanym systemie. Odnosząc się zaś do kolejnych twierdzeń Zamawiającego wykonawca Mirbud stwierdził, że Zamawiający nie raczył wyjaśnić na czym polega wytknięta przez niego „całkowita niespójność”. Nigdzie w SIWZ Zamawiający nie nakazał, ani pośrednio, ani wprost, aby systemy alarmowe (SSWiN, SAP - system sygnalizacji alarmu pożarowego) były systemami tego samego producenta, co system kontroli dostępu firmy UTC. Tym samym zdaniem Odwołującego o jakiegokolwiek sprzeczności pomiędzy ofertą Odwołującego a SIWZ nie może być mowy.

Punkt 1.2 Informacji o odrzuceniu ofert.

Odwołujący wskazywał, że w omawianym zakresie argumentacja Zamawiającego stanowi powielenie jego argumentacji z pkt 1.1. Informacji o odrzuceniu ofert. Ponadto Odwołujący nie zgadzał się z Zamawiającym w kwestii tego jakoby w dokumentacji było wymagane, aby sterownik sieciowy zarządzał 16 kontrolerami. Stwierdził, że w rzeczywistości w dokumentacji wykonawczej wskazano, że: „Sterownik sieciowy będzie zarządzał maksymalnie 16 kontrolerami” (tak w pkt „Sterownik sieciowy”), względnie że: „Każdy ze sterowników sieciowych obsługuje do 16 kontrolerów drzwowych” (tak w pkt „Topologia systemu”). Różnica pomiędzy faktycznym brzmieniem dokumentacji wykonawczej a uzasadnieniem odrzucenia oferty Odwołującego jest więc oczywista i rażąca. W dokumentacji wykonawczej Zamawiający wskazał jedynie iloma kontrolerami maksymalnie będzie zarządzać sterownik sieciowy. Zamawiający nie wymagał, aby sterownik sieciowy zarządzał 16 kontrolerami czy minimum 16 kontrolerami. Zamawiający określił zatem jedynie górną granicę liczby kontrolerów zarządzanych przez sterownik sieciowy. Niewątpliwie centrala ATS (sterownik sieciowy wg nazewnictwa dokumentacji projektowej), do której można podłączyć do 12 kontrolerów, mieści się w określonej przez Zamawiającego górnej granicy liczby kontrolerów zarządzanych przez sterownik sieciowy. W ocenie Odwołującego w pełni dopuszczalna i zgodna z SIWZ jest liczba kontrolerów mniejsza niż maksymalna liczba kontrolerów zarządzanych przez sterownik sieciowy.

Ponadto podkreślał, że w pkt „Topologia systemu” Zamawiający wskazał, że: „Sumarycznie sterownik obsługuje co najmniej 36 czytników”. Biorąc pod uwagę, że do centrali ATS (sterownika sieciowego wg nazewnictwa dokumentacji projektowej) można podłączyć do 12 kontrolerów, a każdy kontroler sieciowy może obsłużyć 4 czytniki, to jak łatwo obliczyć centrala ATS sumarycznie może obsłużyć 48 czytników, czyli znacznie powyżej wymaganego minimum. Co więcej, w zaoferowanym przez Odwołującego systemie kontroli dostępu firmy UTC centrala ATS, oprócz obsługi 48 czytników poprzez 12 kontrolerów, może jeszcze obsłużyć bezpośrednio (bez pośrednictwa kontrolera) 16 czytników. W sumie zatem centrala ATM może obsłużyć 64 czytniki, czyli prawie dwa razy tyle, co minimum wymagane w dokumentacji wykonawczej (36 czytników). Nieprawdziwe jest zatem twierdzenie Zamawiającego zgodnie z którym: „Proponowane rozwiązanie wymusza zwiększenie wymaganej ilości sterowników sieciowych do zaprojektowanej ilości przejść”. Zwiększenie liczby sterowników sieciowych w ogóle nie będzie potrzebne, gdyż jak wskazano powyżej centrala ATS poprzez kontrolery sieciowe może sumarycznie obsłużyć 48 czytników, czyli znacznie więcej niż wymagane

minimum, a dodatkowo może obsłużyć bezpośrednio (bez pośrednictwa kontrolera) 16 czytników. Zdaniem Odwołującego z tego też względu kompletnie chybione i bezprzedmiotowe są dalsze rozważania Zamawiającego co do konsekwencji zwiększenia liczby sterowników sieciowych. Skoro liczba ta nie zwiększy się, to nie wystąpi większe zużycie prądu, nie nastąpi spadek niezawodności systemu, nie będzie konieczności zmian projektu branży elektrycznej jak i nie będzie konieczności koordynacji międzybranżowej. Nie będzie też problemu z miejscem do instalacji dodatkowych urządzeń, gdyż dodatkowych urządzeń po prostu nie będzie. Nie będzie wreszcie zwiększonej liczby akumulatorów a tym samym nie nastąpi zwiększenie kosztów eksploatacyjnych obiektu. W pkt „Topologia systemu” Zamawiający wskazał, że: „Sumarycznie sterownik obsługuje co najmniej 36 czytników”. Natomiast w pkt „Sterownik sieciowy” Zamawiający wskazał, że: „Każdy kontroler podłączony do sterownika sieciowego ma za zadanie obsłużyć nie więcej niż 4 czytniki”. Dzieląc 36 czytników przez 4 czytniki obsługiwane przez pojedynczy kontroler łatwo wyliczyć, że liczba kontrolerów w przypadku 36 czytników wynosi 9. Zatem także sam Zamawiający w dokumentacji wykonawczej zakładał, że do sterownika sieciowego będzie podłączonych 9 kontrolerów, każdy obsługujący nie więcej niż 4 czytniki ($9 \times 4 = 36$). Również z tego względu centrala ATS, która poprzez kontrolery sieciowe może sumarycznie obsłużyć 48 czytników, spełnia wymagania SIWZ.

Punkt 1.3 Informacji o odrzuceniu ofert.

Odnosząc się do twierdzeń Zamawiającego we wskazywanym zakresie Odwołujący stwierdził, że Zamawiający nie wyjaśnił które konkretnie odpowiedzi Odwołującego uznaje za sprzeczne i tym samym za niewiarygodne. W zaoferowanym przez Odwołującego systemie kontroli dostępu firmy UTC kontroler sieciowy działa jako dodatkowy moduł podłączany poprzez interfejs CAN do sterownika sieciowego. Powyższemu w żaden sposób nie zaprzecza fragment wyjaśnień przytoczony przez Zamawiającego. Odwołujący wyjaśniał, że w celu spełnienia powyższego wymagania w systemie kontroli dostępu zostanie zastosowana wtyczka softwarowa na poziomie oprogramowania zarządzającego.

Punkt 1.4 Informacji o odrzuceniu ofert.

Odnosząc się do stwierdzeń Zamawiającego we wskazywanym zakresie Odwołujący podnosił, że jego zdaniem Zamawiający miesza w swoich wywodach dwie zupełnie różne kwestie, tj. wymagania wobec system kontroli dostępu oraz właściwości czytnika ATS1161N.

Zaoferowany przez Odwołującego system kontroli dostępu firmy UTC spełnia wszystkie wymagania określone przez Zamawiającego, w szczególności ma możliwość obsługi protokołu transmisyjnego Wiegand. W opinii Odwołującego w świetle postanowień SIWZ dla zapewnienia zgodności wystarczające jest, aby zaoferowany system kontroli dostępu miał możliwość obsługi (poprzez kontroler drzwiowy) jednego z dwóch protokołów: AbaTRACK II albo Wiegand. System zaoferowany przez Odwołującego taką możliwość posiada, gdyż ma możliwość obsługi (poprzez kontroler drzwiowy) protokołu transmisyjnego Wiegand. Zdaniem Odwołującego z powyższych względów za całkowicie chybione uznać należy wywoływanie Zamawiającego dotyczące uzależnienia użytkownika od jednego typu interfejsu ATS RS-485. Takie uzależnienie nie będzie miało miejsca, gdyż jak wskazano powyżej system zaoferowany przez Odwołującego ma możliwość obsługi (poprzez kontroler drzwiowy) protokołu transmisyjnego Wiegand. Zatem do zaoferowanego systemu można podłączyć i wykorzystać każdy czytnik, który posiada interfejs Wiegand, w tym także czytniki innych producentów. Odwołujący wskazał na powyższe także w złożonych Zamawiającemu wyjaśnieniach z dnia 23 września 2019 r., stwierdzając w nich w pkt 3 i 4, że: „W systemie mogą pracować dowolne czytniki obsługujące interfejs Wiegand”.

Odwołujący przyznał natomiast, że wskazany w wyjaśnieniach z dnia 23 września 2019 r. czytnik ATS1161N nie komunikuje się za pomocą któregośkolwiek ze wskazanych przez Zamawiającego protokołów transmisyjnych: ani Wiegand, ani AbaTrack II. W ocenie Odwołującego zaoferowanie powyższego czytnika stanowi jednak inną omyłkę polegającą na niezgodności oferty z SIWZ, niepowodującą istotnych zmian w treści oferty, którą Zamawiający mógł i powinien poprawić na podstawie art. 87 ust. 2 pkt 3 Pzp. W konsekwencji wystąpienie powyższej omyłki nie uprawniało Zamawiającego do odrzucenia oferty Odwołującego na podstawie art. 89 ust. 1 pkt 2 Pzp. W ocenie Odwołującego w niniejszej sprawie spełnione są wszystkie warunki dopuszczalności poprawienia innej omyłki. Uzasadniając konieczność i dopuszczalność poprawienia omyłki co do czytników Odwołujący wskazywał, że omyłka ta jest konsekwencją wprowadzenia Odwołującego w błąd przez producenta zaoferowanego systemu kontroli dostępu, firmę UTC. Producent, dobierając na etapie składania ofert swoje produkty do wymagań Zamawiającego, wskazał właśnie na czytnik ATS1161N i zapewnił Odwołującego, że czytnik ten spełnia wszystkie wymagania SIWZ. Oczywiście zamiarem Odwołującego było zaoferowanie Zamawiającemu czytnika, który faktycznie spełnia wszystkie wymagania SIWZ, w szczególności komunikuje się za pomocą jednego ze wskazanych przez Zamawiającego protokołów transmisyjnych: Wiegand albo AbaTrack II. Takim czytnikiem jest inny czytnik

produkcji UTC, czyli czytnik ACI407N wraz z interfejsem czytnika Wieganda ATS1170, i na ww. czytnik (wraz z interfejsem czytnika Wieganda ATS1170) Zamawiający mógł i powinien poprawić czytnik wskazany w wyjaśnieniach. O tym, że poprawienie powyższej omyłki jest dopuszczalne, gdyż nie spowoduje istotnych zmian w treści oferty Odwołującego, rozstrzyga szereg względów. Przede wszystkim oba ww. czytniki są czytnikami tego samego producenta, czyli firmy UTC i mogą być używane w ramach zaoferowanego przez Odwołującego systemu kontroli dostępu. Ponadto oba ww. czytniki są do siebie fizycznie bardzo podobne, z punktu widzenia użytkownika różnice między nimi są praktycznie niezauważalne. Również budowa obu ww. czytników jest niemal identyczna, różni je tylko interfejs Wiegand. Czytniki ACI407N jest czytnikiem o tej samej specyfikacji co czytnik ATS1161N, z zastrzeżeniem różnicy dotyczącej interfejsu Wiegand. Także producent traktuje ww. czytniki jako będące swoimi zamiennikami. Cena za ww. czytniki jest praktycznie identyczna i wynosi odpowiednio: w przypadku czytnika ATS1161N - 975 złotych netto a w przypadku czytnika ACI407N (wraz z interfejsem czytnika Wieganda ATS1170) - 973 złotych netto. Zdaniem Odwołującego nie sposób wreszcie nie zauważyć, że jeśli idzie o budowę systemu kontroli dostępu, to czytniki stanowią najmniej istotny element tego systemu, gdyż najłatwiej wymienić je na nowe czy zastąpić zupełnie innymi.

Punkt 1.5 Informacji o odrzuceniu ofert.

Odwołujący stwierdził, że podane przez Zamawiającego uzasadnienie niezgodności treści oferty Odwołującego z treścią SIWZ jest wręcz skrajnie lakoniczne i zdawkowe. Na podstawie stwierdzeń Zamawiającego nie sposób ustalić w jakim konkretnie zakresie i z jakich powodów Zamawiający uznał, iż system kontroli dostępu firmy UTC nie spełnia wymagań SIWZ. Zamawiający nie wskazał bowiem które konkretnie spośród wymaganych przez Zamawiającego funkcjonalności nie są realizowane przez ww. system i dlaczego Zamawiający tak uważa, nie załączył również do swojego pisma informacji uzyskanej od przedstawiciela producenta systemu kontroli dostępu ani nawet nie przytoczył treści tej informacji. Wreszcie Zamawiający w żaden sposób nie wyjaśnił jakie to luki w ochronie obiektu rzekomo spowoduje rozwiązanie zaoferowane przez Odwołującego, z czego te luki miałyby wynikać a przede wszystkim nie wyjaśnił z którymi postanowieniami SIWZ oferta Odwołującego przez owe luki miałyby być sprzeczna i dlaczego. Z tych wszystkich względów jakakolwiek merytoryczna dyskusja ze stanowiskiem Zamawiającego jest niemożliwa, Odwołujący musiałby bowiem zgadywać w jakim zakresie i z jakich względów Zamawiający uznał treść oferty Odwołującego za niezgodną z treścią SIWZ. Tak zdawkowe uzasadnienie odrzucenia oferty Odwołującego uniemożliwia jemu

ustalenie jakie były konkretnie powody odrzucenia jego oferty i tym samym uniemożliwia odniesienie się do tych powodów w odwołaniu. Samo przytoczenie przez Zamawiającego fragmentu dokumentacji wykonawczej niczego tutaj nie wyjaśnia i nie stanowi wymaganego przepisami uzasadnienia faktycznego. Dlatego też Odwołujący może jedynie ogólnie stwierdzić, że zaoferowany przez niego system kontroli dostępu firmy UTC spełnia wszystkie wymagania SIWZ, w szczególności spełnia wszystkie wymagania zawarte w dokumentacji wykonawczej. Zamawiający w żaden sposób nie wykazał, że jest inaczej. Odwołujący wnosił o pominięcie przez Izbę wszelkich dodatkowych powodów odrzucenia oferty Odwołującego, podanych przez Zamawiającego w toku postępowania odwoławczego a które nie zostały podane przez niego w Informacji o odrzuceniu ofert. W szczególności dotyczyć to będzie tych powodów, które wynikają z informacji uzyskanej przez Zamawiającego od przedstawiciela producenta systemu kontroli dostępu, gdyż powody te nie zostały wskazane w Informacji o odrzuceniu ofert.

Punkt 2 Informacji o odrzuceniu ofert.

Wykonawca Mirbud podał, że odnośnie zaoferowanego przez niego systemu monitoringu obiektowego CCTV firmy HIKVISION POLAND Sp. z o.o. Zamawiający podniósł w szereg zarzutów. W ocenie Odwołującego wszystkie te zarzuty Zamawiającego wynikają z zasadniczego nieporozumienia i niewłaściwej interpretacji złożonych przez niego wyjaśnień treści oferty. Zamawiający najwyraźniej przyjął, że zaoferowany przez Odwołującego system monitoringu obiektowego składać się będzie wyłącznie z oprogramowania klienckiego iVMS-4200, dekodera DS-6900 oraz rejestratora Hikvision. Takie założenie jest błędne i bezpodstawne. W złożonych wyjaśnieniach Odwołujący skupił się na ustosunkowaniu się do wszystkich zarzutów podniesionych w przesłanych mu przez Zamawiającego zastrzeżeniach wniesionych przez wykonawcę ALSTAL Grupa Budowlana sp. z o.o. sp.k. (dalej: „Przystępujący”), a nie na opisywaniu całości systemu monitoringu obiektowego CCTV firmy HIKVISION POLAND Sp. z o.o. Zamawiający w wezwaniu do wyjaśnień z dnia 16 września 2019 r. wskazał wyraźnie, że takiego właśnie ustosunkowania się oczekuje. Zamawiający nie zażądał natomiast od Odwołującego kompleksowej i wyczerpującej informacji na temat budowy i elementów składowych systemu monitoringu obiektowego CCTV.

Odwołujący wyjaśniał, że wskazane w wyjaśnieniach oprogramowanie iVMS4200, dekodery z serii DS-6900UDI oraz rejestrator Hikvision mają służyć jedynie obsłudze systemu interkomowego, natomiast zarządzanie i obsługa systemu CCTV będzie się odbywać poprzez oprogramowanie HIKCENTRAL firmy HIKVISION POLAND Sp. z o.o. Innymi słowy w

zaoferowanym systemie rejestracja dźwięku z terminali interkomowych, zsynchronizowanego z obrazem z niezależnej kamery obsługiwanej przez system CCTV na serwerach systemu CCTV w paśmie nie mniejszym niż 7 kHz oraz metodą kompresji G.722, jest realizowana poprzez zastosowanie dekodera z serii DS-6900UDI, rejestratora Hikvision oraz oprogramowania iVMS4200, dzięki któremu jest możliwa współpraca z oprogramowaniem HIKCENTRAL. Wykorzystanie oprogramowania iVMS4200 i oprogramowania HIKCENTRAL powoduje, że wbrew twierdzeniom Zamawiającego zaoferowany system zapewnia integrację programową platformy CCTV z zaprojektowanym systemem interkomowym. Oprogramowanie HIKCENTRAL pracujące w architekturze Klient-Serwer, oparte jest o rozwiązanie serwerowe i posiada różne interfejsy komunikacyjne, jak również jest otwarte na integrację z produktami innych producentów. Poprzez oprogramowanie HIKCENTRAL system CCTV będzie miał możliwość komunikacji poprzez ogólnodostępny protokół IP/SIP.

Za kompletnie chybione i bezpodstawne Odwołujący uważał zarzuty Zamawiającego dotyczące dekodera z serii DS-6900UDI. Zamawiający zarzucił Odwołującemu, że: „Dekoder nie posiada parametrów odpowiadających terminalom interkomowym, a zastosowanie rejestratora całkowicie wyklucza funkcjonalność systemu wyspecyfikowanego w zamówieniu. Na podstawie analizy przesłanej przez wykonawcę karty katalogowej DS-6900UDI SERIES DECODER Zamawiający jednoznacznie stwierdza, że urządzenie nie posiada możliwości komunikacji z protokołem IP/SIP - cytując z dokumentacji wykonawczej: „Należy zastosować serwery wraz z oprogramowaniem o parametrach nie gorszych niż: - Zarejestrowani subskrybenci: IP/SIP: maks. 64". Wymagane było w dokumentacji wykonawczej, aby system CCTV miał możliwość komunikacji poprzez ogólnodostępny protokół IP/SIP. Natomiast załączona do wyjaśnień Wykonawcą karta katalogowa DS-6900UDISERIES DECODER nie ma wymaganego protokołu transmisji". W rozwiązaniu zaoferowanym przez Odwołującego dekodery nie jest terminalem interkomowym i już tylko z tego względu nie musi posiadać parametrów wymaganych w przypadku terminala interkomowego. Jeżeli natomiast Zamawiającemu chodziło o to, że parametry dekodera są takie, iż uniemożliwiają współpracę dekodera z terminalami interkomowymi, to stwierdzenie powyższe zdaniem Odwołującego jest nieprawdziwe i pozbawione podstaw. W złożonej ofercie, ani w złożonych wyjaśnieniach Odwołujący nie wskazał (gdyż nie miał takiego obowiązku) jaki model terminala interkomowego oferuje. Zatem Zamawiający nie był i nie jest w stanie porównać parametrów dekodera i terminala interkomowego a tym bardziej stwierdzić ich niezgodności. Kompletnie chybiony jest również zarzut, że dekodery nie posiada możliwości komunikacji z protokołem IP/SIP. W opinii

Odwołującego w świetle postanowień dokumentacji projektowej dekodery takiej możliwości mieć nie musi, co jasno i wyraźnie wynika z przytoczonego przez Zamawiającego fragmentu dokumentacji wykonawczej. Zresztą sam Zamawiający słusznie wskazał, że „Wymagane było w dokumentacji wykonawczej, aby system CCTV miał możliwość komunikacji poprzez ogólnodostępny protokół IP/SIP”. W zaoferowanym przez Odwołującego systemie możliwość komunikacji poprzez ogólnodostępny protokół IP/SIP zapewnia oprogramowanie HIKCENTRAL, na co już wskazano powyżej. Tym samym wymagania dokumentacji projektowej są spełnione. Równie bezpodstawne są zarzuty Zamawiającego dotyczące rejestratora. Zamawiający zarzucił, że: „(...) zastosowanie rejestratora całkowicie wyklucza funkcjonalność systemu wyspecyfikowanego w zamówieniu”, a dalej w tym samym punkcie rozwinął powyższy zarzut, wskazując, że: „Proponowane przez MIRBUD S.A. rozwiązanie oparte o rejestratory powoduje brak możliwości wykorzystania zaawansowanych funkcjonalności kamer innych producentów niż producent rejestratora”. Odwołujący wyjaśniał, że w zaoferowanym systemie dekodery z serii DS-6900UDI, rejestrator Hikvision oraz oprogramowanie iVMS4200 są wykorzystywane wyłącznie do rejestracji dźwięku z terminali interkomowych, zsynchronizowanego z obrazem z niezależnej kamery obsługiwanej przez system CCTV na serwerach systemu CCTV w paśmie nie mniejszym niż 7 kHz oraz metodą kompresji G.722. Natomiast zgodnie z wymaganiami dokumentacji projektowej w zaoferowanym systemie kamery będą obsługiwane przez system CCTV na serwerach systemu CCTV. Powyższą obsługę kamer będzie zapewniać oprogramowanie HIKCENTRAL, pracujące w architekturze Klient-Serwer i oparte o rozwiązanie serwerowe. Zdaniem Odwołującego z analogicznych względów za chybione i bezpodstawne uznać należy zarzuty Zamawiającego dotyczące oprogramowania iVMS-4200. Zamawiający zarzucił, że: „Zaproponowane oprogramowanie iVMS-4200 jest oprogramowaniem klienckim używanym do zarządzania rejestratorami, a nie oprogramowaniem, które będzie pełniło rolę serwera tak rozbudowanego systemu CCTV. (...) Ponadto rozwiązanie nie będzie stanowiło wymaganego w dokumentacji projektowej jednolitego systemu CCTV opartego na strukturze klient - serwer, a składać się będzie z kilku systemów współpracujących za pomocą tylko oprogramowania klienckiego”. Odwołujący wyjaśniał ponownie, że wskazane w wyjaśnieniach oprogramowanie iVMS4200, dekodery z serii DS-6900UDI oraz rejestrator Hikvision mają służyć jedynie obsłudze systemu interkomowego, natomiast zarządzanie i obsługa systemu CCTV będzie się odbywać poprzez oprogramowanie HIKCENTRAL firmy HIKVISION POLAND Sp. z o.o. Oprogramowanie HIKCENTRAL pracuje w architekturze Klient-Serwer, oparte jest o rozwiązanie serwerowe i to ono będzie pełniło rolę

serwera systemu CCTV. Tym samym oferowany system stanowi wymagany w dokumentacji projektowej jednolity system CCTV, oparty na strukturze Klient - Serwer. Odwołujący stwierdził, że wszystkie sformułowane przez Zamawiającego zarzuty dotyczące oprogramowania klienckiego iVMS-4200, dekodera DS-6900 i rejestratora HIKVISION oceniać należy jako całkowicie chybione.

Ad II.

Odwołujący podnosił, że przedstawione przez Zamawiającego uzasadnienie niezgodności treści oferty Odwołującego z treścią SIWZ jest wręcz skrajnie lakoniczne i zdawkowe i uniemożliwia ustalenie jakie były konkretnie powody odrzucenia jego oferty i tym samym uniemożliwia odniesienie się do tych powodów w odwołaniu. Jakakolwiek merytoryczna dyskusja ze stanowiskiem Zamawiającego jest niemożliwa, Odwołujący musiałby bowiem zgadywać w jakim zakresie i z jakich względów Zamawiający uznał treść oferty Odwołującego za niezgodną z treścią SIWZ. Zdaniem Odwołującego z uzasadnienia podanego przez Zamawiającego nie sposób dowiedzieć się ani z którymi konkretnie postanowieniami SIWZ oferta Odwołującego jest rzekomo sprzeczna, ani dlaczego Zamawiający uznał, że ta rzekoma sprzeczność w ogóle zachodzi. Odwołujący zauważał, że nie będzie dopuszczalne „uzupełnienie” przez Zamawiającego wskazanych powyżej braków uzasadnienia faktycznego odrzucenia oferty Odwołującego poprzez wskazanie ich w odpowiedzi na odwołanie czy w trakcie rozprawy przez Krajową Izbę Odwoławczą. Wszystkie informacje w tym zakresie winny zostać podane przez Zamawiającego w piśmie informującym o odrzuceniu oferty Odwołującego.

Ad III.

Odwołujący wskazywał, że powyższy zarzut podnosi wyłącznie z ostrożności procesowej, tj. na wypadek gdyby Izba uznała, że argumenty i dowody przedstawione przez Odwołującego w odwołaniu oraz w toku postępowania odwoławczego nie są wystarczające do stwierdzenia, że treść oferty Odwołującego odpowiada treści SIWZ. W przypadku, gdy Zamawiający poweźmie jakiegokolwiek wątpliwości co do treści złożonej oferty, może żądać od wykonawcy stosownych wyjaśnień. Wyjaśnienia mogą dotyczyć wszystkich elementów oferty, zarówno jej zawartości merytorycznej, jak i warunków wykonania zamówienia. Skoro zatem Zamawiający powziął wątpliwość w zakresie zgodności treści oferty złożonej przez Odwołującego z treścią SIWZ, to Zamawiający mógł i powinien te wątpliwości wyjaśnić.

Zamawiający w każdym z punktów Informacji o odrzuceniu ofert wytknął Odwołującemu, że wykonawca w piśmie z dnia 23 września 2019 r. nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia jego wymagania. Odwołujący podkreślał, że jeżeli w ocenie Zamawiającego złożone przez Odwołującego wyjaśnienia nie były wystarczające, to w żaden sposób nie oznacza to niezgodności treści oferty Odwołującego z treścią SIWZ i w żadnym wypadku nie uprawnia Zamawiającego do odrzucenia oferty Odwołującego. Zamawiający mógł i powinien w takim wypadku wezwać Odwołującego do złożenia dodatkowych wyjaśnień, wskazując w wezwaniu, czego w pierwszych wyjaśnieniach mu zabrakło i do czego Odwołujący powinien się jeszcze odnieść. Zamawiający dopuścił się natomiast bezpodstawnego i bezprawnego uproszczenia, uznając, że brak jednoznacznego wyjaśnienia danej kwestii i poparcia wyjaśnień dowodami oznacza niezgodność treści oferty Odwołującego z treścią SIWZ. Tymczasem brak taki, jeżeli w ogóle miał miejsce, oznacza co najwyżej niedoskonałość złożonych wyjaśnień i powoduje potrzebę wezwania do ich złożenia po raz kolejny. Nie ma jednak żadnych przeszkód, a jest wręcz konieczne, aby Zamawiający zwrócił się do Odwołującego o wyjaśnienia w tym zakresie w toku ponownego badania i oceny ofert. Z uwagi na fakt, że Zamawiający zaniechał dalszego dopytania o zaoferowane przez Odwołującego systemy, które błędnie ocenił jako niezgodne z treścią SIWZ, zdaniem Odwołującego stwierdzić należy, że Zamawiający naruszył przepis art. 87 ust. 1 Pzp przez zaniechanie wyjaśnienia zakresów oferty Odwołującego, które zdaniem Zamawiającego stanowiły podstawę do jej odrzucenia, gdyż błędnie wyłożył treść oferty Odwołującego i treść dotyczących jej wyjaśnień, co w rezultacie doprowadziło do jej bezprawnego odrzucenia.

Stanowisko Zamawiającego.

Zamawiający odpowiedział na odwołanie wskazując, że podtrzymuje swoją decyzję o odrzuceniu oferty Odwołującego. W uzasadnieniu prezentowanego stanowiska Zamawiający podnosił, że w jego ocenie, wspartej opinią autora dokumentacji projektowej, tj. firmy ENDUSTRIA PROJECT sp. z o.o., przyjęte w ofercie Odwołującego rozwiązania w zakresie budowy systemu kontroli dostępu (SKD) budynku oraz systemu monitoringu wizyjnego (CCTV) - nie spełniają wymagań technicznych, określonych w dokumentacji projektowej, stanowiącej załącznik do SIWZ w przedmiotowym przetargu.

Niezgodność systemu kontroli dostępu (SKD).

Zamawiający podnosił, że Odwołujący w odwołaniu (str. 14) przyznał, że w wyjaśnieniach z dnia 23 września 2019 r. przywołany czytnik nr ATS 1161N nie komunikuje się ze wskazanymi przez Zamawiającego protokołami transmisyjnymi: ani Wiegand ani AbaTrack II, co oznacza, że oferowane czytniki są zupełnie bezużyteczne dla Zamawiającego. W konsekwencji wykonawca żąda od Zamawiającego poprawienia omyłki na podstawie art. 87 ust. 2 pkt 3 Pzp. Zamawiający nie zgadzał się z przytoczonymi argumentami z następujących powodów. W celu ewentualnego poprawienia rzekomej omyłki, służby techniczne Zamawiającego musiałyby dokonać analizy technicznej wszystkich czytników firmy UTC pod kątem, który z nich:

- spełnia wymagania techniczne określone w SIWZ, w szczególności, które komunikują się z protokołami Wiegand/AbaTrack II,
- jest nieprzydatny do wbudowania w budynku KPP Piła z innych technicznych przyczyn,
- jest zgodny z innymi rozwiązaniami dokumentacji projektowej i zapewni pełną przydatność do obsługi policjantów, pracowników cywilnych zatrudnionych w KPP Piła i osób trzecich współpracujących z Policją.

Analiza techniczna, o której mowa powyżej i dokonanie wyboru przez Zamawiającego właściwego czytnika spośród wielu dostępnych czytników, w celu poprawienia rzekomej omyłki nie jest rolą Zamawiającego i taka czynność może wiązać się z technicznym ryzykiem niewłaściwego doboru. W celu ewentualnego poprawienia rzekomej omyłki, Zamawiający musiałby podjąć negocjacje z wykonawcą w zakresie: po pierwsze ustalenia właściwego czytnika, po drugie zmiany oferty wykonawcy Mirbud (zamiana czytnika ATS 1161N na czytnik np. ACI 407N lub jeszcze inny czytnik) co nie jest dopuszczalne na gruncie art. 87 ust. 1 ustawy, bowiem nie jest możliwe prowadzenie negocjacji między Zamawiającym i wykonawcą dotyczącej złożonej ceny, a wyjaśnienia nie mogą zmieniać treści oferty. Ponadto Zamawiający musiałby ustalić, jaka jest różnica w cenie oferowanych czytników, aby ustalić wpływ ich zmiany i wyceny na cenę oferty. Wszystkie przytoczone powyżej argumenty świadczą o tym, że rzekomy błąd w doborze systemu kontroli dostępu i jego elementów nie jest omyłką, o której mowa w art. 87 ust. 2 pkt 3 ustawy, polegającą nie niezgodności oferty ze specyfikacją niepowodującą istotnych zmian w treści oferty, którą poprawia Zamawiający powiadamiając o tym wykonawcę - z następujących względów:

- prawdą jest, że w ofercie nastąpiła niezgodność z SIWZ ale, aby Zamawiający mógł poprawić ową niezgodność musiałby w treści oferty zauważyć treść, którą mogły bez większych trudności wprowadzić/zamienić w ofercie bez dodatkowych ustaleń z wykonawcą, negocjacji czy analiz technicznych,
- Zamawiający nie może ustalić istotności wprowadzonych zmian,
- Zamawiający uzyskał wiedzę o właściwym typie czytnika, który prawdopodobnie spełniałby założenia projektowe, w celu rzekomego poprawienia omyłki w ofercie Mirbud, dopiero w wyniku złożenia odwołania, a we wcześniejszej korespondencji między stronami kwestia ta nie była w ogóle podniesiona co dowodzi również braku cech omyłki w rozumieniu powyżej przywołanego przepisu Pzp.

Zamawiający wskazywał, że zupełnie nie akceptuje twierdzenia Odwołującego, że „to czytniki stanowią najmniej istotny element tego systemu, gdyż najłatwiej wymienić je na nowe czy zastąpić zupełnie innym”. Zgoda na proponowaną praktykę wyboru oferty z wadą w doborze urządzeń, a następnie zmiana wadliwych elementów oferty na właściwe np. na etapie przetargu lub na etapie budowy jest nie tylko naganna z punktu widzenia realizacji zamówień publicznych, ale niesie za sobą ryzyka prawnokarne (zmiana urządzeń lub elementów systemu w stosunku do oferty - zarzut działania na niekorzyść Skarbu Państwa), finansowe (ryzyka niewłaściwej wyceny, tj. umniejszenia i zwiększenia ceny o zmienione czytniki), techniczne (ryzyko niewłaściwego działania czytników, tj. niezgodnie z dokumentacją projektową), prawne (naruszenie praw autorskich dokumentacji projektowej) i inne.

Zamawiający stwierdził, że Odwołujący bagatelizuje w odwołaniu kwestię czytników systemu kontroli dostępu, twierdząc, że jest to najmniej istotny element oferty. W ocenie Zamawiającego kwestia dostępu do budynku i jego właściwej ochrony, pracy w budynku dla 357 policjantów i pracowników Policji, kwestia dostępu przede wszystkim dla obywateli i społeczeństwa, a także innych osób współpracujących z Policją (prokuratura, KAS i inne organy) nie jest bagatelna. System musi być właściwie dobrany, szczelny i pod ścisłą kontrolą służb technicznych Policji, bez szkody dla jego działania, późniejszych awarii, niekompatybilności z innymi systemami, bez ryzyka dodatkowych kosztów, które poniósłby inwestor związanych z technicznymi uszkodzeniami lub nefunkcjonowaniem systemu. Zamawiający wyjaśniał, że Komenda Powiatowa Policji w Pile stanowi centralny ośrodek Policji w powiecie pilskim, ale jak każda komenda Policji współpracuje też z innymi jednostkami Policji w Wielkopolsce ale i w całym kraju. W jednostkach Policji prowadzone są śledztwa i dochodzenia nie tylko o lokalnej skali, ale również w wymiarze wojewódzkim, a nawet

międzynarodowym z udziałem prokuratury i innymi organami. Zdarzają się próby przejścia grup przestępczych przez system ochronny budynków Policji, próby kradzieży dowodów rzeczowych z magazynów dowodów, próby podpaleń jednostek Policji, podkładane są materiały wybuchowe w jednostkach Policji, ataki na dyżurnych przy pomocy noży, siekier i inne zdarzenia o charakterze przestępczym. W odniesieniu do ww. przytoczonych argumentów, system kontroli dostępu i czytników nie jest dla Policji sprawą błahą i bagatelną, jak to wyraża Odwołujący, ale istotną z punktu widzenia sprawności i profesjonalizmu pracy organów ścigania oraz właściwej ochrony przed przenikaniem grup przestępczych.

Następnie Zamawiający wskazał, że na stronie 15 odwołania wykonawca Mirbud wyjaśnił, że przyczyną niewłaściwego doboru czytników było wprowadzenie w błąd przez producenta systemu kontroli dostępu firmę UTC. Zgodnie z art. 429 Kc kto powierza wykonanie czynności drugiemu, ten jest odpowiedzialny za szkodę wyrządzoną przez sprawcę przy wykonywaniu powierzonej mu czynności, zatem wykonawca Mirbud jako profesjonalista ponosi konsekwencje niewłaściwego doboru systemu i jego elementów poprzez powierzenie tego doboru innemu podmiotowi gospodarczemu, zatem wina w wyborze, o której mowa w art. 429 k.c. obciąża wykonawcę, a nie Zamawiającego. W odwołaniu wykonawca Mirbud żądał naprawy przez Zamawiającego szkody (poprawienie rzekomej omyłki), która nastąpiła z winy wykonawcy i podmiotu któremu powierzył dobór systemu kontroli dostępu i jego elementów podczas, gdy zgodnie z art. 415 k.c. szkodę naprawia ten, kto ją wyrządził.

Następnie Zamawiający podnosił, że do odpowiedzi na odwołanie załączył wyciąg z dokumentacji projektowej, w którym projektant branży teletechnicznej określił rozwiązanie projektowe w zakresie kontroli dostępu, przy czym:

- w wyjaśnieniach z dnia 23 września 2019 r. pojawia się rozwiązanie zupełnie odmienne od zaprojektowanego (cyt. str. 5 - „Każdy z kontrolerów posiada swoją lokalną kopię bazy danych użytkowników i bufor zdarzeń, który pozwala na synchronizację zdarzeń po ponownym połączeniu z centralą i systemem zarządzającym. Łączna pojemność gałęzi systemu obsługiwanej przez jedną centralę to 48 drzwi. Każdy kontroler dysponuje własną pamięcią z bazą użytkowników i buforem zdarzeń”).
- w odwołaniu zaś pojawia się rozwiązanie zupełnie odmienne od zaprojektowanego i odmienne w stosunku do wyjaśnień z dnia 23 września 2019 r. (cyt. str. 7 – „każda centrala ATS (sterownik sieciowy wg nazewnictwa dokumentacji projektowej) posiada własny monitorowany zasilacz buforowy, pełną bazę danych użytkowników i ich uprawnień oraz rejestr zdarzeń”).

Zdaniem Zamawiającego te same funkcje w wyjaśnieniach są przypisane kontrolerowi, a w odwołaniu centrali ATS - sprzeczność wyjaśnień - powodując tym samym zmiany w stosunku do pierwotnych założeń o charakterze technicznym nie tylko niejednoznaczne, ale i powodujące konieczność przeprojektowania dokumentacji projektowej przez Zamawiającego wraz z wyliczeniami inżynierskimi, gdyby hipotetycznie Zamawiający tę ofertę wybrał jako najkorzystniejszą, po wcześniejszym ustaleniu z wykonawcą Mirbud, która z tych wersji jest wiążąca, co jest niedopuszczalne na podstawie Pzp i procesem inwestycyjnym. Konieczność przeprowadzenia wyliczeń matematycznych wynika ze strony 74 dokumentacji projektowej - załącznik nr 2 (projektant wyliczył obciążenia prądowe w jednostce mA, czasy podtrzymania i inne dla sterowników, a nie dla centrali).

Zamawiający, opierając się na treści dokumentacji projektowej wskazał, że system dostępu winien być zbudowany ze sterowników sieciowych, do których zostaną podłączone następne urządzenia systemu. Wykonawca Mirbud w odwołaniu wskazuje, że zamiast sterowników sieciowych wskazanych w dokumentacji projektowej będą montowane centrale ATS - podmiana urządzeń w stosunku do dokumentacji projektowej, w ocenie Zamawiającego jest niedopuszczalna z tego względu, że narusza strukturę dokumentacji projektowej i w sposób nieuprawniony zmienia rozwiązania projektowe, bez uzgodnień z projektantem, niepoparte wyliczeniami (napięcia, natężenia prądu, moc elektryczna urządzeń dla całego systemu i w całym budynku, współistnienie z innymi systemami teletechnicznymi). Przy podmianie sterowników sieciowych na centrale należy przeprojektować instalację elektryczną, wentylację i system klimatyzacji, a na tym etapie przetargu i na etapie budowy obiektu nie jest to możliwe (dwukrotne projektowanie i wydatkowanie środków na dodatkowe opracowania projektowe). Tłumaczenia wykonawcy Mirbud w odwołaniu, że „Zamawiający nie zakazał łączenia w jednym urządzeniu funkcji sterowników sieciowych i central alarmowych” są bezzasadne. Powtarzanie kilkakrotnie tego argumentu dla każdej wprowadzonej zmiany technicznej w ofercie Mirbud w stosunku do projektu, stanowi naruszenie art. 22 ust. 3 prawa budowlanego, zgodnie z którym kierownik budowy (przedstawiciel wykonawcy na budowie) zapewnia zorganizowanie budowy i kierowanie budową obiektu budowlanego w sposób zgodny z projektem. To, że Zamawiający niczego „nie zakazał”, nie oznacza, że wykonawca Mirbud może wprowadzać samodzielnie zmiany do projektu. Takie tłumaczenie, w istocie narusza cały przebieg procesu budowlanego i obowiązki poszczególnych uczestników tego procesu, określone w prawie budowlanym (przeprojektowanie projektu - projektant, nadzór autorski i odpowiedzialność projektanta głównie branży teletechnicznej ale i projektantów pozostałych branż, inwestora -

Zamawiającego - dodatkowa płatność za przeprojektowanie projektu, zmiany techniczne na budowie - zamiana materiałów budowlanych i urządzeń, opóźnienia w budowie itp.). Zamawiający stwierdził, że wykonawca oświadczył, w ofercie, że opiera się na rozwiązaniach zgodnych z dokumentacją projektową, bez rozwiązań równoważnych, a tymczasem stosuje rozwiązania inne niż wskazane w tej dokumentacji (np. centrala ATS zamiast sterownik), w ocenie Zamawiającego, niezgodne z dokumentacją projektową.

Zamawiający wyjaśniał, że w dokumentacji projektowej wymagał zaoferowania systemu kontroli dostępu w oparciu o interfejs CAN (w załączeniu wyciąg z dokumentacji projektowej str. 71. Interfejs CAN (informatyce i elektronice interfejs to urządzenie pozwalające na połączenie ze sobą dwóch (lub więcej) innych urządzeń, które bez niego nie mogłyby ze sobą współpracować). CAN charakteryzuje się dużą odpornością na zakłócenia i niezawodnością. Tymczasem wykonawca Mirbud zamiast interfejsu CAN oferuje interfejs RS485. W pkt 12 odwołania wykonawca Mirbud. wskazuje że cyt.: „kontroler sieciowy działa jako dodatkowy moduł podłączony poprzez Interfejs CAN do sterownika sieciowego”, co oznacza chyba, że będzie wbudowany interfejs RS 485 i interfejs CAN, poprzez dodatkowe urządzenie - co jeszcze bardziej spowalnia pracę systemu. Można bowiem połączyć oba interfejsy, ale poprzez dodatkowe urządzenie, a tego dokumentacja projektowa nie przewiduje, w przeciwnym razie po raz kolejny należy zmieniać dokumentację, poszczególne rysunki, dokonać przeliczeń zużycia prądu itd. Reasumując Zamawiający stwierdził, że zaproponowany interfejs RS485 jest niezgodny z dokumentacją projektową ze wszystkimi konsekwencjami wynikającymi odpowiednio z uzasadnienia w pkt 2.9. i pkt 2.10. Zamawiający podkreślał, że oba interfejsy działają zupełnie odmiennie. Interfejs RS485 spowalnia pracę systemu bowiem działa kilkadziesiąt razy wolniej niż interfejs CAN, dlatego, że interfejs RS komunikuje się z modułami „odpytując” je po kolei, natomiast w przypadku interfejsu CAN moduł samodzielnie przesyła informacje do centrali głównej (bez odpytywania modułów po kolei jak w RS), a moduły jednocześnie wysyłają rejestracje.

Systemu monitoringu wizyjnego CCTV:

Zamawiający wyjaśniał, że na stronie 60 dokumentacji projektowej Zamawiający określił, że system CCTV składa się z:

1. dwóch rodzajów kamer,
2. stacji klienckiej,

3. serwerów oraz oprogramowania o wymaganych funkcjonalnościach.

Odwołując się do elementów systemu określonych w pkt 1 do 3 dokłada jeszcze: dodatkowe oprogramowanie IVMS4200 oraz dekodery z serii DS - 6900UDI oraz rejestrator Hikvision, aby uzyskać wymagane funkcjonalności. Zamiast tych dwóch urządzeń oraz oprogramowania wykonawca Mirbud winien zaoferować serwer interkomowy. Zmiana serwera interkomowego na dekoder, rejestrator i dodatkowe oprogramowanie to rozwiązanie techniczne po raz kolejny niezgodne z dokumentacją projektową o poważnych konsekwencjach technicznych. Zastosowanie proponowanego przez wykonawcę Mirbud rozwiązania rodzi następujące skutki:

- brak rysunków technicznych projektowych dla montażu dodatkowych dwóch urządzeń systemu wbudowanego w budynku uniemożliwia prowadzenie budowy systemu CCTV w budynku Komendy Policji w Pile,
- możliwe kolizje techniczne i zakłócenia z innymi systemami (instalacją elektryczną, wentylacją, klimatyzacją, systemem kontroli dostępu, BMS, siecią strukturalną, systemem włamania i napadu, sygnalizacji alarmu pożarowego, systemem łączności radiowej sieci i systemy są od siebie zależne w całości lub części, współpracują ze sobą),
- nieaktualność wyliczeń projektanta dla wartości pobranej mocy dobranych urządzeń, poboru prądu, czasu podtrzymania urządzeń i inne, w związku z powyższym istnieje konieczność dokonania dodatkowych przeliczeń i istnieje ryzyko zmiany dobranych urządzeń,
- naruszenie praw autorskich autora dokumentacji projektowej i wykluczenie jego odpowiedzialności zawodowej za szkody wobec inwestora za nieuprawnione wprowadzenie zmian do projektu,
- wzrost kosztów po stronie Zamawiającego konieczność rewizji dokumentacji projektowej a nawet jej przeprojektowania i wzrost kosztów nadzoru autorskiego, szacowane przez Zamawiającego na poziomie około 100 000 zł, dalsze koszty zmian technicznych trudne do przewidzenia,
- konieczność dostosowania sposobu użytkowania obiektu do nowych dodatkowych urządzeń, co powoduje wzrost kosztów eksploatacji (systemu CCTV w jednostkach Policji w Wielkopolsce od wielu lat budowane i remontowane są w oparciu o serwery).

Zamawiający podnosił, że ze względów określonych powyżej (podpalenia, wybuchy, przenikanie przestępców, kradzieże dowodów rzeczowych z jednostek Policji, ataki z użyciem niebezpiecznych narzędzi i inne zdarzenia o charakterze kryminalnym), system monitoringu

wizyjnego, a więc system kamer, rejestracji zapisu z kamer, archiwum danych na serwerach, słowem system obserwacji budynków, ich przestrzeni wokół lub wewnątrz budynków musi działać w sposób oczekiwany przez Policję, w sposób uzgodniony wcześniej przez inżynierów Policji z projektantami danego budynku, a nie w sposób narzucony przez wykonawcę w ofercie. Należy też dodać, że dzięki zapisom archiwalnym z systemu CCTV (w wyniku działania systemu w sposób oczekiwany przez Policję) szybko udało się ująć np. sprawców podpalenia Komendy Policji w Lesznie oraz zidentyfikować nożownika z Rybnika.

Zmiany poczynione przez wykonawcę Mirbud w ofercie w zakresie czytników (zmiana oświadczenia wykonawcy), zmiany wprowadzone w zakresie systemu CCTV (dodatkowe dwa urządzenia oraz dodatkowe oprogramowanie), zmiany w systemie kontroli dostępu (zamiana sterowników na centrale, zmiana interfejsów) stanowią, w ocenie Zamawiającego, ofertę z zastrzeżeniem zmiany, o którym mowa w art. 68 § 1 i §2 k. c., zgodnie z którą - § 1 - w stosunkach między przedsiębiorcami odpowiedź na ofertę z zastrzeżeniem zmian lub uzupełnień niezmieniających istotnie treści oferty poczytuje się za jej przyjęcie. W takim wypadku strony wiąże umowa o treści określonej w ofercie, z uwzględnieniem zastrzeżeń zawartych w odpowiedzi na nią. § 2 art. 68 k.c. nie stosuje się, jeżeli w treści oferty wskazano, że może ona być przyjęta jedynie bez zastrzeżeń albo, gdy oferent niezwłocznie sprzeciwił się włączeniu zastrzeżeń do umowy, albo gdy druga strona w odpowiedzi na ofertę uzależniła jej przyjęcie od zgody oferenta na włączenie zastrzeżeń do umowy, a zgody tej niezwłocznie nie otrzymała. Zamawiający w postępowaniach o zamówienia publiczne oczekuje oferty bez zastrzeżenia jej zmiany lub uzupełnień, a ewentualne zmiany treści oferty mogą wynikać ściśle z przepisów Pzp, co w przedmiotowej sprawie nie ma miejsca.

Zamawiający podał, że posiadał wiedzę, że oferowane w ofercie Mirbud systemy teletechniczne nie spełniają wymagań technicznych dokumentacji projektowej już w dniu złożenia oferty, a nie w wyniku złożenia przez Mirbud wyjaśnień w trybie art. 87 ust. 1 Pzp. Zamawiający stosuje taką praktykę przy udzielaniu zamówień publicznych, że przed planowanym wykluczeniem wykonawcy lub odrzuceniem oferty umożliwia wykonawcy wypowiedzenie się w spornych kwestiach w celu umożliwienia wykonawcom podjęcia obrony swojej oferty. Skierowanie zapytania do wykonawcy Mirbud o wyjaśnienie kwestii technicznych oferowanych systemów wskazuje, że Zamawiający widzi niezgodności w ofercie, w przeciwnym razie w przypadku braku wątpliwości ze strony Zamawiającego, zapytanie o wyjaśnienia nie byłoby kierowane do wykonawcy Mirbud. Oświadczenie Firmy Projektowej Industria Project sp. z o.o. z dnia 17 września 2019 r. na zapytanie Zamawiającego potwierdza, że Zamawiający

posiadł wątpliwości co do niezgodności oferty z projektem odpowiednio wcześniej, niż w dniu złożenia wyjaśnień przez wykonawcę Mirbud.

Następnie Zamawiający wyjaśniał, że Komenda Wojewódzka Policji w Poznaniu prowadziła i prowadzi szereg inwestycji budowlanych na terenie Wielkopolski, w których są wbudowywane systemy teletechniczne różnych producentów. Zamawiający prowadząc proces inwestycyjny, począwszy od wytycznych do koncepcji projektowej i dokumentacji projektowej, na odbiorach końcowych robót skończywszy, kontroluje i ujednolica systemy wbudowywane w obiektach Policji woj. wielkopolskiego (w Wielkopolsce znajduje się jest około 500 budynków Policji). W tym celu Zamawiający dobiera kompatybilne systemy kontroli dostępu i kompatybilne systemu CCTV w pełni nowoczesne, uwzględniając swoje potrzeby wynikające z działalności statutowej, uwzględniając zagrożenia, analizując koszty budowy i użytkowania systemów i w oparciu o ich funkcjonalności buduje lub remontuje obiekty Policji w Wielkopolsce. Wykonawca Mirbud zaproponował systemy, które nie odpowiadają wymaganiom technicznym Inwestora.

Wraz z odpowiedzią na odwołanie Zamawiający złożył następujące dokumenty:

1. załącznik nr 1 - oświadczenie projektanta,
2. załącznik nr 2 - wyciąg z dokumentacji projektowej - wyliczenia techniczne zasilania systemu kontroli dostępu,
3. załącznik nr 3 - wyciąg z dokumentacji projektowej - opis budowy systemu CCTV,
4. załącznik nr 4 - informacja o podpaleniu KMP Leszno, podłożeniu bomby w KP Kłodawa, atak nożownika w Komendzie w Rybniku,
5. załącznik nr 5 - wyciąg z dokumentacji projektowej schemat i rysunek systemu kontroli dostępu.

Uwzględniając treść dokumentacji postępowania o udzielenie zamówienia przekazanej przez Zamawiającego, dowody oraz stanowiska i oświadczenia Stron oraz Przystępującego, złożone w pismach procesowych i na rozprawie, Izba ustaliła co następuje.

Zamawiający w Załączniku nr 1 specyfikacji, stanowiący wzór Formularza ofertowego, w części A w pkt 1 sprecyzował, że oczekuje podania ceny ofertowej za wykonanie przedmiotu zamówienia zgodnie z załączonym zestawieniem kosztów oraz przy użyciu materiałów:

- a) wynikających z dokumentacji wykonawczej

- b) równoważnych zgodnie z załączonymi do oferty dokumentami*
* niepotrzebne skreślić lub usunąć

Odwołujący w złożonej ofercie w Formularzu ofertowym w części A w pkt 1a precyzyjnie wskazał, że oferuje wykonanie przedmiotu zamówienia przy użyciu materiałów wynikających z dokumentacji wykonawczej stanowiącej załącznik do SIWZ. Odwołujący w treści ww. Formularza wykreślił treść wskazującą, że oferuje wykonanie przedmiotu zamówienia przy użyciu materiałów równoważnych zgodnie z załączonymi dokumentami.

Wykonawca Mirbud w złożonej ofercie (str. 1 i 2 Formularza ofertowego) zaoferował między innymi:

- 5) wykonanie systemu kontroli dostępu producenta UTC Fire&Securite Sp. z o.o.
- 7) wykonanie systemu monitoringu obiektowego CCTV producenta HIKVISION POLAND Sp. z o.o.

W dniu 13 września 2019 r. do Zamawiającego zostały przesłane przez Przystępującego zastrzeżenia do oferty Odwołującego w zakresie zaoferowanych przez tego wykonawcę systemów.

W dniu 16 września 2019 r. Zamawiający na podstawie art. 87 ust. 1 Pzp zwrócił się do wykonawcy Mirbud o złożenie stosownych wyjaśnień, w tym: „(...)

1. rzetelne ustosunkowanie się do wszystkich zarzutów podniesionych w zastrzeżeniach pod kątem spełniania wymagań w Państwa ofercie w odniesieniu do założeń określonych w dokumentacji wykonawczej;
2. techniczne uzasadnienie dobranych w Państwa ofercie systemów w stosunku do zarzutów wniesionych przez ALSTAL, które pozwolą Zamawiającemu na uznanie poprawności Państwa oferty, sprawny wybór najkorzystniejszej oferty, uniknięcie sporów arbitrażowych i sądowych, podpisanie umowy o roboty budowlane;
3. ewentualne załączenie do wyjaśnień dokumentów - dowodów, w szczególności od producentów spornych systemów, które pozwolą Zamawiającemu na rzetelną i obiektywną ocenę Państwa oferty.

Jednocześnie informuję, że żądane przez Zamawiającego wyjaśnienia nie mogą prowadzić do zmiany treści Państwa oferty, pod rygorem jej odrzucenia. (...)

W wyznaczonym terminie wykonawca Mirbud złożył Zamawiającemu żądane wyjaśnienia a wraz z nimi następujące następujące dokumenty:

1. Karta katalogowa dla oprogramowania systemu HIKVISION – iVMS-4200 wraz z tłumaczeniem na język polski,
2. Karta katalogowa dla dekodatorów z serii DS-6900UDI wraz z tłumaczeniem na język polski,
3. Karta katalogowa dla systemu kontroli dostępu opartego o zintegrowane centrale ATS Advisor Advanced,
4. Karta katalogowa dla ATS1251 - Modułu kontroli dostępu dla 4 drzwi,
5. Karta katalogowa zintegrowanego systemu bezpieczeństwa,
6. Oferta kompleksowa DGT sp. z o.o. na system łączności radiowej,
7. Karta katalogowa czytnika kart zbliżeniowych.

W piśmie z dnia 30 września 2019 r. pt. Informacja o odrzuceniu ofert Zamawiający wskazał, że po przeprowadzeniu analizy złożonych przez wykonawcę Mirbud wyjaśnień, w oparciu o własną wiedzę i doświadczenie, dostępne źródła informacji o systemach, opinie producentów systemów oraz opinię biura projektowego, które opracowało dokumentację wykonawczą, stanowiącą szczegółowy opis przedmiotu uznał, że oferta w zakresie powyżej określonych systemów nie spełnia wymagań SIWZ, określonych w rzeczonyj dokumentacji i podlega odrzuceniu na podstawie art. 89 ust. 1 pkt 2 Pzp.

Zamawiający podniósł, że wymagał wskazania w Formularzu ofertowym producentów systemów, które spełnią wszystkie wymagania techniczne i funkcjonalne określone w dokumentacji wykonawczej, która stanowiła załącznik nr 5 do SIWZ. Zaś wykonawca Mirbud wskazał w ofercie, że zamierza realizować zadanie przy użyciu materiałów wynikających z dokumentacji wykonawczej, skreślając jednocześnie możliwość wykorzystania rozwiązań równoważnych.

Zdaniem Zamawiającego powyżej określone systemy oferowane w przez wykonawcę Mirbud nie spełniają następujących wymagań dokumentacji wykonawczej, tj.

„1. MIRBUD S.A. w formularzu ofertowym w pkt 5 części A wskazał, że wykona system kontroli dostępu oparty o rozwiązania firmy UTC Fire&Securite Sp. z o.o. Oferowany system kontroli dostępu nie spełnia niżej wymienionych parametrów, które były opisane w dokumentacji wykonawczej. (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych

wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. Przedstawiony załącznik nr 3 wyjaśnień, na który się powołuje MIRBUD S.A. w opisie dotyczy oprogramowania integrującego ATS różne systemy. Natomiast załącznik nie przedstawia dowodu na spełnienie w/w wymagania, tj. zapewnienia inteligencji rozproszonej do poziomu lokalnych sterowników. Zamawiający wymagał budowy systemu kontroli dostępu w oparciu o sterowniki sieciowe wraz z kontrolerami sieciowymi i serwerem dedykowanym do kontroli dostępu. Natomiast Wykonawca wykazuje, że zamierza wybudować system składający się z central ATS, które będą również pełnić funkcje central alarmowych. Takie rozwiązanie powoduje zmniejszenie niezawodności systemu. Proponowane rozwiązanie oparto o wykorzystanie fizycznego interfejsu RS485, który jest przestarzały i nie stosowany w nowoczesnych systemach kontroli dostępu. Wykorzystanie tego interfejsu spowoduje wolniejszą niż projektowana pracę urządzeń w tak rozbudowanym systemie (np. aktualizacja uprawnień dla użytkowników w kontrolerach może zostać wydłużona kilkukrotnie). Również awaria central spowoduje wyłączenie obu systemów, co jest dla Zamawiającego niedopuszczalne. Poza tym MIRBUD S.A. w formularzu ofertowym wykazał, że systemy alarmowe (SSWiN, SAP) zamierza wykonać przy wykorzystaniu rozwiązań innych producentów niż UTC, co jest całkowicie niespójne.

1.2. Wymagania dokumentacji projektowej:

Sterownik sieciowy (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. Zamawiający wymagał budowy systemu kontroli dostępu w oparciu o sterowniki sieciowe wraz z kontrolerami sieciowymi i serwerem dedykowanym do kontroli dostępu. Natomiast MIRBUD S.A. wykazuje, że zamierza wybudować system składający się z central ATS, które będą również pełnić funkcje central alarmowych. Wykorzystanie urządzeń do dwóch systemów kontroli dostępu i alarmu, jak w odpowiedzi wykazał Wykonawca, spowoduje znaczny spadek niezawodności systemów. Poza tym MIRBUD S.A. wykazał, że do centrali alarmowej można podłączyć do 12 kontrolerów, natomiast w dokumentacji jest wymagane aby sterownik sieciowy zarządzał 16 kontrolerami. Proponowane rozwiązanie wymusza zwiększenie wymaganej ilości sterowników sieciowych do zaprojektowanej ilości przejść. Dodatkowa liczba urządzeń pracujących w trybie całodobowym spowodowałaby większe zużycie prądu oraz spadek niezawodności systemu. Zwiększona ilość urządzeń wymusza konieczność zmian projektu branży elektrycznej (każdy z kontrolerów wymaga doprowadzenia instalacji zasilającej oraz zasilacza buforowego wraz z akumulatorem) oraz koordynacji międzybranżowej (nie ma

gwarancji, że w zaprojektowanym obiekcie znajdą się miejsca do instalacji dodatkowych urządzeń). Zwiększona ilość akumulatorów spowoduje zwiększenie kosztów eksploatacyjnych obiektu.

1.3. Wymagania dokumentacji projektowej:

Kontroler sieciowy (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. W odpowiedzi na pytanie dotyczące topologii systemu udzielił wyjaśnień, że wewnętrzna gałąź okablowania kontrolerów wykorzystuje fizycznie interfejs RS485, a nie wymagany CAN. Takie sprzeczne odpowiedzi nie są wiarygodne.

1.4 Wymagania dokumentacji projektowej:

„Czytniki (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. Wykonawca w odpowiedzi z dnia 23.09.2019 r. przedstawił kartę katalogową czytnika ATS1161N, z której wynika, że nie spełnione są bardzo ważne wymagania dotyczące możliwości podłączenia szerokiego zakresu czytników. Wymagane było w dokumentacji projektowej, aby system kontroli dostępu miał możliwość komunikacji z czytnikami w różnych ogólnodostępnych protokołach. W projekcie wymagane było aby system miał możliwość obsługi protokołów transmisyjnych: Wiegand, AbaTrack II. Natomiast załączona do wyjaśnień Wykonawcy karta katalogowa czytnika ATS1161N nie ma wymaganych protokołów transmisyjnych.

W karcie katalogowej czytnika ATS1161N widnieje informacja, że czytnik posiada wyłącznie interfejs ATS RS-485, co jest niezgodne z wymaganiami opisu przedmiotu zamówienia. Dla Zamawiającego zastosowanie oferowanego rozwiązania jest niedopuszczalne ze względu na fakt, iż powoduje to uzależnienie użytkownika od jednego typu interfejsu ATS RS-485 (stosowanego przez wyłącznie jednego producenta), co w przypadku zaprzestania jego produkcji spowoduje konieczność wymiany całego systemu kontroli dostępu.

1.5. Wymagania dokumentacji projektowej:

„Realizowane funkcje (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. Załączył jedynie opis produktu zintegrowany system bezpieczeństwa, telewizyjny

system nadzoru, system sygnalizacji włamania, system kontroli dostępu, system sygnalizacji pożaru, aplikacja zarządzająca, z którego nie wynika, że proponowany w ofercie system kontroli dostępu będzie realizował wymagane funkcje opisane w dokumentacji projektowej. Ponadto Zamawiający uzyskał informację od przedstawiciela producenta systemu kontroli dostępu UTC, że ich rozwiązania nie realizują wszystkich wymaganych przez Zamawiającego funkcjonalności. Zaprojektowany system kontroli dostępu ma zapewniać bezpieczeństwo budynku Komendy Powiatowej Policji w Pile, który wymaga szczególnej ochrony zabezpieczającej przed dostępem osób nieuprawnionych. Zaoferowane przez firmę MIRBUD S.A. rozwiązanie spowoduje niedopuszczalne przez Zamawiającego luki w ochronie obiektu.

2. MIRBUD S.A. w formularzu ofertowym w pkt 7 części A wskazał, że wykona system monitoringu obiektowego CCTV oparty o rozwiązania firmy HIKVISION POLAND Sp. z o.o. Oferowany system monitoringu obiektowego nie spełnia niżej wymienionych parametrów, które były opisane w dokumentacji projektowej. (...) MIRBUD S.A. w piśmie z dnia 23.09.2019 nie przedstawił jednoznacznych wyjaśnień i dowodów, potwierdzających, że oferowany system spełnia w/w wymagania. Zaproponowane rozwiązanie HIKVISION nie spełnia w/w wymienionych funkcjonalności. Proponowany przez MIRBUD S.A. system nie zapewnia integracji programowej platformy CCTV z zaprojektowanym systemem interkomowym co wyklucza ich współdziałanie, a tym samym eliminuje wymaganą funkcjonalność w użytkowaniu. Przedstawiona przez MIRBUD S.A. karta katalogowa dotyczy oprogramowania klienckiego iVMS-4200 i nie dowodzi spełnienia wymaganej w dokumentacji projektowej funkcjonalności „komunikacja dwukierunkowa pomiędzy serwerami systemu CCTV oraz systemu komunikacji głosowej”. Brak takiej funkcjonalności jest niedopuszczalny dla Zamawiającego, np. utrudni policjantom na stanowisku kierowania jednostką sprawne zarządzanie dostępem do obiektu. W rozwiązaniu HIKVISION przedstawionym przez MIRBUD S.A. opisano zastosowanie dekodera DS-6900 oraz rejestratorów. Dekoder nie posiada parametrów odpowiadających terminalom interkomowym, a zastosowanie rejestratora całkowicie wyklucza funkcjonalność systemu wyspecyfikowanego w zamówieniu. Na podstawie analizy przesłanej przez Wykonawcę karty katalogowej DS-6900UDI SERIES DECODER Zamawiający jednoznacznie stwierdza, że urządzenie nie posiada możliwości komunikacji z protokołem IP/SIP - cytując z dokumentacji wykonawczej:

„Należy zastosować serwery wraz z oprogramowaniem o parametrach nie gorszych niż:
- Zarejestrowani subskrybenci: IP/SIP: maks. 64”

Wymagane było w dokumentacji wykonawczej, aby system CCTV miał możliwość komunikacji poprzez ogólnodostępny protokół IP/SIP. Natomiast załączona do wyjaśnień Wykonawcę karta katalogowa DS-6900UDI SERIES DECODER nie ma wymaganego protokołu transmisji. Dla Zamawiającego zastosowanie oferowanego rozwiązania jest niedopuszczalne ze względu na fakt, iż powoduje to uzależnienie użytkownika od jednego typu rozwiązania interkomowego producenta HIKVISION (stosowanego przez wyłącznie jednego producenta), co w przypadku zaprzestania jego produkcji spowoduje konieczność wymiany całego systemu. Zaproponowana przez Wykonawcę topologia nie spełnia wymagań opisanych w dokumentacji wykonawczej:

„Zaprojektowano system zbudowany w architekturze klient-serwer”.

„System CCTV oparty o serwer i kamery stanowi zintegrowaną platformą IP. Platforma zapewnia możliwość zarządzania zdarzeniami ze stanowiska kierowania. System składa się z urządzeń w postaci serwerów wizyjnych oraz kamer IP.” Zaproponowane oprogramowanie iVMS-4200 jest oprogramowaniem klienckim używanym do zarządzania rejestratorami, a nie oprogramowaniem, które będzie pełniło rolę serwera tak rozbudowanego systemu CCTV. Proponowane przez MIRBUD S.A. rozwiązanie oparte o rejestratory powoduje brak możliwości wykorzystania zaawansowanych funkcjonalności kamer innych producentów niż producent rejestratora. Ponadto rozwiązanie nie będzie stanowiło wymaganego w dokumentacji projektowej jednolitego systemu CCTV opartego na strukturze klient serwer, a składać się będzie z kilku systemów współpracujących za pomocą tylko oprogramowania klienckiego. Rozwiązanie MIRBUD S.A. powoduje dla użytkownika utrudnienia w nadzorowaniu, zarządzaniu oraz konserwacji systemu.

Reasumując, uznanie oferty MIRBUD S.A. za ważną, dokonanie jej wyboru jako najkorzystniejszej, w następstwie powierzenie temu Wykonawcy budowy Komendy Powiatowej Policji w Pile według oferowanych rozwiązań technicznych spowoduje następujące konsekwencje:

1. budowa obiektu budowlanego nastąpi w sposób niezgodny i sprzeczny z SIWZ, w tym niezgodnie z dokumentacją projektową
2. naruszy zasadę uczciwej konkurencji i równego traktowania Wykonawców w odniesieniu, szczególnie do tych podmiotów, które zaoferowały prawidłowe systemy, kosztem wyższej ceny za budowę obiektu,
3. doprowadzi do wbudowania systemów niefunkcjonalnych - nieuwzględniających specyfiki budynków Policji w zakresie bezpieczeństwa, nadzorowania i zarządzania —

pomimo, że od wielu lat i w wielu budynkach Policji stosuje się rozwiązania nowoczesne i funkcjonalne w wieloletniej perspektywie rozwoju,

4. spowoduje wbudowanie systemów nieenergooszczędnych, przez oferowanie wielu urządzeń w stosunku do projektowanego, co zwiększa koszty zużycia energii, kosztów zarządzenia i eksploatacji,
5. ograniczy możliwość rozbudowy obiektu o następne systemy bezpieczeństwa i nadzoru wyłączanie do jednego producenta tych systemów, co może przełożyć się bezpośrednio na wysoki koszt ich dokupienia, w przypadku zaistnienia takiej potrzeby (serwisowanie, gwarancja, utrzymanie systemu po upływie gwarancji i rękojmi, wymiana części zamiennych), przy czym należy dodać, że założeniem projektowym Zamawiającego jest zakup systemów otwartych na inne marki i produkty w przyszłość”.

Izba zważyła co następuje.

Na wstępie Krajowa Izba Odwoławcza stwierdza, że Odwołujący legitymuje się uprawnieniem do korzystania ze środków ochrony prawnej, o którym stanowi przepis art. 179 ust. 1 Pzp, według którego środki ochrony prawnej określone w ustawie przysługują wykonawcy, uczestnikowi konkursu, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów niniejszej ustawy.

W toku rozprawy zostały złożone następujące dowody:

1. Oświadczenie firmy Hikvision Poland Sp. z o.o. z siedzibą w Warszawie opatrzone datą 21.10.2019 r. w którym, podano m. in., że: „W odpowiedzi na Państwa zapytanie dotyczące spełnienia wymagań dokumentacji przetargowej w postępowaniu jak powyżej informujemy, że firma Hikvision posiada w swojej ofercie zarówno urządzenia obiektowe oraz komercyjne oprogramowanie pozwalające Państwu na zrealizowanie instalacji systemu CCTV jak również integracji z systemami firm trzecich w zgodzie z wymaganiami dokumentacji”.
2. Korespondencja w formie e-mail pomiędzy Panem A.W. pracownikiem Zamawiającego a W.W. przedstawicielem firmy UTC Fire&Securite Sp. z o.o. wraz z załącznikiem.

Analiza zarzutów podniesionych w treści odwołania doprowadziła skład orzekający Izby do przekonania, że odwołanie podlega oddaleniu.

Przytaczając, zgodnie z wymaganiami art. 196 ust. 4 Pzp, przepisy stanowiące podstawę prawną zapadłego rozstrzygnięcia, a których naruszenie przez Zamawiającego zarzucił Odwołujący, wskazać należy, że zgodnie z art. 7 ust. 1 Pzp Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób zapewniający zachowanie uczciwej konkurencji i równe traktowanie wykonawców oraz zgodnie z zasadami proporcjonalności i przejrzystości.

Zgodnie z art. 89 ust. 1 pkt 2 Pzp Zamawiający odrzuca ofertę jeżeli jej treść jest nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt 3 Pzp. Natomiast według art. 87 ust. 2 pkt 3 ustawy Zamawiający poprawia w ofercie omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty.

Zaś przepis z art. 87 ust. 1 Pzp stanowi, że w toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Niedopuszczalne jest prowadzenie między zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty oraz, z zastrzeżeniem ust. 1a i 2, dokonywanie jakiegokolwiek zmiany w jej treści.

Zgodnie z art. 92 ust. 1 pkt 3 Pzp Zamawiający informuje niezwłocznie wszystkich wykonawców o: wykonawcach, których oferty zostały odrzucone, powodach odrzucenia oferty, a w przypadkach, o których mowa w art. 89 ust. 4 i 5, braku równoważności lub braku spełniania wymagań dotyczących wydajności lub funkcjonalności - podając uzasadnienie faktyczne i prawne.

Kluczowym zagadnieniem, wysuwającym się na czoło w niniejszej sprawie, jest konieczność rozstrzygnięcia kwestii, związanej z tym, czy treść oferty wykonawcy Mirbud odpowiada treści specyfikacji, a jeśli nie, czy podlega odrzuceniu na podstawie art. 89 ust. 1 pkt 2 Pzp. Izba uznała, że na tak zadane pytanie należy udzielić odpowiedzi twierdzącej.

W zakresie rozstrzygnięcia zgłoszonych zarzutów istotnym jest, że Odwołujący w złożonej ofercie, w Formularzu ofertowym w części A w pkt 1a, jasno i precyzyjnie wskazał, że oferuje wykonanie przedmiotu zamówienia przy użyciu materiałów wynikających z dokumentacji wykonawczej, stanowiącej załącznik do SIWZ. Odwołujący w treści ww. formularza wykreślił treść wskazującą, że oferuje wykonanie przedmiotu zamówienia przy użyciu materiałów równoważnych zgodnie z załączonymi dokumentami. Wyżej opisane ustalenia Izby w zakresie rezygnacji wykonawcy Mirbud z przedstawienia rozwiązań równoważnych w złożonej ofercie zostały również potwierdzone przez Odwołującego nie tylko w złożonych wyjaśnieniach z dnia 23 września 2019 r. (str. 1 i 2 wyjaśnień) ale również w toku rozprawy. W kontekście powyższego za rozstrzygające dla zasadności zgłoszonych zarzutów należy uznać rozwiązania techniczne wskazane w treści dokumentacji wykonawczej, stanowiącej w tym przypadku podstawę do badania treści oferty Odwołującego wraz ze złożonymi wyjaśnieniami w zakresie wskazanych w tych dokumentach rozwiązań.

Izba odnosiła się szczegółowo do poszczególnych kwestii, które stanowiły istotę ww. zarzutów.

1.1. System kontroli dostępu – topologia systemu.

Nie było sporne między stronami, że w dokumentacji wykonawczej, która stanowiła załącznik do SIWZ w Tomie: II Projekt Architektoniczno-Budowlany Budynek A, w części: VI Branża Teletechniczna, 2.4.8 System kontroli dostępu (str. 70) podano: „Topologia systemu. Aby zabezpieczyć bezproblemowe działanie zaprojektowanego systemu, na wypadek braku komunikacji lub uszkodzenia serwera, inteligencja musi zostać rozproszona do poziomu lokalnych sterowników. Każdy ze sterowników sieciowych obsługuje do 16 kontrolerów drzwiowych a każdy kontroler drzwiowy co najmniej 4 czytniki. Sumarycznie sterownik obsługuje co najmniej 36 czytników”.

Wykonawca Mirbud w wyjaśnieniach z dnia 23 września 2019 r. podał m. in.: „Jedna gałąź systemu kontroli dostępu UTC Fire & Security obsługuje 48 drzwi inteligentnych i do 16 drzwi podstawowych, łącznie można w gałęzi podłączyć 112 czytników, część czytników może być dublowana (z zachowaniem identyfikacji czytników) łącznie daje to ilość 208 czytników. Wewnątrz gałęzi okablowanie kontrolerów wykorzystuje fizycznie interfejs RS485, który może być przesyłany również przy wykorzystaniu sieci Ethernet. System posiada szeroki wachlarz akcesoriów umożliwiającą elastyczną realizację okablowania – rozgałęźniki, izolatory, itp. W zakresie kontroli dostępu zaoferowaliśmy system oparty o zintegrowane centrale ATS Advisor

Advanced (Załącznik nr 3). Topologia systemu zakłada, że centrala alarmowa jest jednocześnie sterownikiem kontroli dostępu. Zapewnia to stosowną autonomię – baza użytkowników wraz z uprawnieniami alarmowymi i kontroli dostępu jest wspólna dla obu systemów – zapewnia to pracę obu systemów bez połączenia z systemem zarządzającym w razie utraty połączenia. Do zaoferowanej centrali alarmowej można podłączyć do 12 kontrolerów obsługujących 4 przejścia, mogą one być zarówno jednostronne jak i dwustronne. Każdy z kontrolerów posiada swoją lokalną kopię bazy danych użytkowników i bufor zdarzeń, który pozwala na synchronizację zdarzeń po ponownym połączeniu z centralą i systemem zarządzającym. Łączna pojemność gałęzi systemu obsługiwanej przez jedną centralę to 48 drzwi. Każdy kontroler dysponuje własną pamięcią z bazą użytkowników i buforem zdarzeń. Brak wzajemnych połączeń centrali/sterownika sieciowego i kontrolera nie wyłącza systemu i można z niego swobodnie korzystać. Bufor w każdym z urządzeń zapewnia ponowną synchronizację zdarzeń po przywróceniu połączenia”.

W świetle powyżej zacytowanych wymogów dokumentacji wykonawczej - o którą zgodnie z oświadczeniem Odwołującego, zawartym w pkt 1a w Formularza ofertowego, powinny zostać oparte rozwiązania zaoferowane przez wykonawcę Mirbud - uznać należy, że system kontroli dostępu w dokumentacji wykonawczej został zaprojektowany w oparciu o urządzenia takie jak sterowniki. W dokumentacji przewidziano, że każdy ze sterowników sieciowych obsługuje do 16 kontrolerów drzwiowych a każdy kontroler drzwiowy co najmniej 4 czytniki. Sumarycznie sterownik obsługuje co najmniej 36 czytników. W kontekście powyższego za niezgodne z wymaganiami specyfikacji należy uznać zaoferowanie przez Odwołującego rozwiązania, opierającego się na zastosowaniu central alarmowych ATS zamiast sterowników.

Izba nie dała wiary wyjaśnieniom Odwołującego, zawartym w odwołaniu i powielonym w toku rozprawy, iż wskazywane centrale ATS nie będą pełniły funkcji central alarmowych, lecz będą wyłącznie sterownikami sieciowymi. Odwołujący w toku rozprawy twierdził, że centrale ATS mogą spełniać dwie funkcjonalności jednocześnie, tj. kontroli dostępu i centrali kontroli dostępu. Mogą również spełniać ww. funkcjonalności odrębnie. Izba wskazuje, że powyższe twierdzenia stoją w oczywistej sprzeczności z powołanymi powyżej wyjaśnieniami Odwołującego zawartymi w piśmie z dnia 23 września 2019 r. (pkt 1 str. 5 i pkt 2 str. 6 wyjaśnień), w którym Odwołujący nie wskazał, że centrale alarmowe będą pełniły rolę sterowników a wprost i jednoznacznie stwierdził, że topologia systemu zakłada, że centrala alarmowa jest jednocześnie sterownikiem kontroli dostępu. Wydaje się oczywiste, że konsekwencją zaoferowanego przez Odwołującego rozwiązania opierającego się o centrale alarmowe ATS jest niespełnienie

wymogu Zamawiającego, wynikającego z dokumentacji wykonawczej, tj. zapewnienia inteligencji rozproszonej do poziomu lokalnych sterowników. W ocenie Izby powyższego nie obalają również twierdzenia Odwołującego, który wskazywał, że Formularzu ofertowym w pkt 6 wskazał, że oferuje wykonanie systemu sygnalizacji włamania i napadu producenta SATEL sp. z o.o. W kontekście powyższego należy jedynie przyznać rację Zamawiającemu, który stwierdził, że oferta Odwołującego i złożone przez niego wyjaśnienia są niespójne.

1.2. System kontroli dostępu – sterownik sieciowy

W dokumentacji wykonawczej podano: „Sterownik sieciowy - Elementami wykonawczymi systemu kontroli dostępu będą sterowniki sieciowe. Sterowniki będą podłączone do sieci LAN za pomocą standardu TCP/IP. W przypadku zerwania łączności kontrolera sieciowego z serwerem, będzie on nadal zarządzać elementami do niego podłączonymi. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja. Sterownik sieciowy będzie zarządzał maksymalnie 16 kontrolerami, do których będzie doprowadzony interfejs CAN. Każdy kontroler podłączony do sterownika sieciowego ma za zadanie obsłużyć nie więcej niż 4 czytniki. Sam sterownik sieciowy również obsługuje do 2 przejść jedno lub dwustronnych”.

W wyjaśnieniach z dnia 23 września 2019 r. wykonawca Mirbud podał m. in.: „Każda gałąź systemu kontroli dostępu UTC Fire&Security połączona jest do jednostki centralnej szyfrowanym kanałem z wykorzystaniem sieci Ethernet. Każdy kontroler dysponuje własną pamięcią z bazą użytkowników i buforem zdarzeń. Brak wzajemnych połączeń centrali/sterownika sieciowego i kontrolera nie wyłącza systemu i można z niego swobodnie korzystać. Bufor w każdym z urządzeń zapewnia ponowną synchronizację zdarzeń po przywróceniu połączenia. Topologia systemu zakłada, że centrala alarmowa jest jednocześnie sterownikiem kontroli dostępu. Zapewnia to stosowną autonomię – baza użytkowników wraz z uprawnieniami alarmowymi i kontroli dostępu jest wspólna dla obu systemów – zapewnia to pracę obu systemów bez połączenia z systemem zarządzającym w razie utraty połączenia. Do centrali alarmowej można podłączyć do 12 kontrolerów obsługujących 4 przejścia, mogą one być zarówno jednostronne jak i dwustronne. Każdy z kontrolerów posiada swoją lokalną kopię bazy danych użytkowników i bufor zdarzeń, który pozwala na synchronizację zdarzeń po ponownym połączeniu z centralą i systemem zarządzającym. Łączna pojemność gałęzi systemu obsługiwanej przez jedną centralę to 48 drzwi. Jedna gałąź zaoferowanego systemu kontroli dostępu UTC Fire & Security obsługuje 48 drzwi inteligentnych i do 16 drzwi podstawowych,

łącznie można w gałęzi podłączyć 112 czytników, część czytników może być dublowana (z zachowaniem identyfikacji czytników), co łącznie daje 208 czytników”.

Rozstrzygnięcie zarzutu wymaga odpowiedzi na pytanie, czy w świetle treści dokumentacji wykonawczej należy uznać, że Zamawiający ustanowił obligatoryjny wymóg zaoferowania rozwiązania przewidującego zarządzaniem przez sterownik sieciowy maksymalnie 16 kontrolerami co oznacza, że w ofercie w tym zakresie należy przewidzieć rozwiązanie na 16 kontrolerów, czy też dopuszczalne było posłużenie się rozwiązaniem przewidującym zarządzanie przez sterownik sieciowy 12 kontrolerów jako rozwiązaniem, które uwzględnia maksymalną liczbę kontrolerów? Analiza całości dokumentacji postępowania na którą składa się również dokumentacja wykonawcza doprowadziła Izbę do wniosku, że wymaganym przez Zamawiającego było zaoferowanie rozwiązania, które uwzględniałoby zarządzanie przez sterownik sieciowy 16 a nie 12 kontrolerami. Izba w tym zakresie przyznała rację Przystępującemu, który powoływał się na treść dokumentacji wykonawczej, w której na stronie 69 podano, że Zamawiający przewiduje sukcesywną rozbudowę systemu kontroli dostępu. Tym samym Izba stwierdziła, że wykonawca przy projektowaniu oferowanych rozwiązań powinien uwzględnić tę okoliczność a nie jedynie opierać się na stanie dotychczasowym. Zatem zasadnym i niezbędnym jest, aby zaoferowane przez wykonawcę rozwiązanie uwzględniało to, że sterownik sieciowy może zarządzać maksymalnie 16 kontrolerami. Tego wymogu nie spełnia rozwiązanie zaproponowane przez Odwołującego, bowiem do wskazanej przez wykonawcę Mirbud centrali alarmowej można podłączyć jedynie do 12 kontrolerów. Biorąc pod uwagę powyższe należy uznać za zasadne stwierdzenie Zamawiającego, że tego rodzaju rozwiązanie, które oferuje Odwołujący wymusza konieczność zmiany projektu branży elektrycznej a także prawdopodobnym jest, że może powodować w przyszłości zwiększenie kosztów eksploatacyjnych.

Izba za nietrafne uznała twierdzenia Odwołującego, oparte o treść dokumentacji wykonawczej na str. 73 pt. „Zasilanie”, z której wykonawca Mirbud wywodził, że dobór urządzeń powinien mieć miejsce dopiero na późniejszym terminie, tj. na etapie realizacji zamówienia. Izba wskazuje, że w powoływanym przez Odwołującego zakresie dokumentacja stanowi, że: „Zasilanie. Zasilanie sterowników oraz kontrolerów odbywać się będzie przez zasilacze buforowe 230VAC/12VDC, które mają za zadanie podtrzymać działanie kontroli dostępu w razie zaniku zasilania na 12 godzin. Poniżej przedstawiono obliczenia do doboru akumulatorów. Na etapie wykonania, po ostatecznym po ostatecznym doborze urządzeń należy ponownie przeprowadzić obliczenia uwzględniając wartość pobranej mocy dobranych urządzeń”.

Izba stanęła na stanowisku, że z powołanej treści dokumentacji wykonawczej Odwołujący wywodzi błędne wnioski, bowiem jej treść opisuje przypadek mający na celu weryfikację związaną z ponownym przeprowadzeniem obliczeń, uwzględniających wartość pobranej mocy przez zastosowane urządzenia. Wcale nie oznacza to, że wykonawca ubiegający się o udzielenie zamówienia nie ma obowiązku doboru i zaoferowania w złożonej ofercie odpowiednich urządzeń, spełniających wymagania określone przez Zamawiającego treścią specyfikacji, przy czym wskazać powinien, czy oferuje rozwiązania oparte o dokumentację wykonawczą, czy też równoważne, a w takim przypadku powinno to mieć to odzwierciedlenie w złożonych dokumentach. Należy też uznać za trafne stwierdzenie Przystępującego, że w celu kalkulacji ceny przyjętej w złożonej ofercie koniecznym był dobór konkretnych urządzeń z uwagi na fakt występowania w ramach prowadzonego postępowania rozwiązań, które są dla niego dedykowane, a zatem są „szyte na miarę”.

Izba wskazuje również na niekonsekwentne stanowisko Odwołującego w zakresie informacji zawartych w kartach katalogowych, załączonych do wyjaśnień. Z jednej strony wykonawca Mirbud przekłada ww. karty jako dokumenty mające potwierdzać spełnienie wymagań postawionych przez Zamawiającego przez oferowane rozwiązania wskazane w ofercie Odwołującego a z drugiej strony dyskredytuje informacje w nich zawarte stwierdzając, że są to jedynie podstawowe informacje, które nie mogą stanowić miarodajnego źródła, które może służyć potwierdzeniu stanowiska prezentowanego przez Odwołującego w zakresie oferowanych rozwiązań.

1.3 System kontroli dostępu – kontroler sieciowy.

Nie było sporne między stronami, że treścią dokumentacji wykonawczej Zamawiający sprecyzował, że: „Kontroler sieciowy - Kontroler sieciowy działa jako dodatkowy moduł podłączany poprzez interfejs CAN do sterownika sieciowego. Obsługuje on jedno lub dwa przejścia jedno lub dwustronne. Projektowany kontroler drzwiowy musi obsługiwać do czterech czytników kontroli dostępu i komunikować się z nimi za pomocą protokołów AbaTRACK II/Wiegand. W zależności od typu architektury kontroler musi oferować wejścia i wyjścia do podłączenia elementów wykonawczych (kontaktronów, zwór, elektrozaczepów, przycisków wyjścia, czy przycisków ewakuacyjnych). Kontrolery drzwiowe wyposażone w akumulator 7Ah pozwalające na podtrzymanie zasilania przez 12 godzin”.

Izba ustaliła, że w złożonych wyjaśnieniach z dnia 23 września 2019 r. wykonawca Mirbud wskazał m. in. że: „W zaoferowanym systemie kontroli dostępu UTC Fire & Security znajduje się m.in. interfejs CAN i każda centrala i kontroler dysponuje monitorowanym zasilaczem buforowym, które można doposażyć w akumulatory 7-18-26Ah lub więcej i w zależności od obciążenia (zwory, zamki, inne akcesoria) zapewniają one autonomię zasilania na nawet 60h pracy. Do centrali alarmowej można podłączyć do 12 kontrolerów obsługujących 4 przejścia, mogą one być zarówno jednostronne jak i dwustronne. Każdy z kontrolerów posiada swoją lokalną kopię bazy danych użytkowników i bufor zdarzeń, który pozwala na synchronizację zdarzeń po ponownym połączeniu z centralą i systemem zarządzającym. Łączna pojemność gałęzi systemu obsługiwanej przez jedną centralę to 48 drzwi. Wszystkie powyższe informacje znajdują potwierdzenie w Załączniku nr 4. W systemie mogą pracować dowolne czytniki obsługujące interfejs Wiegand. Zaoferowaliśmy wykorzystanie czytników zintegrowanych w systemie ATS1160/61N pracujących z dwukierunkową magistralą systemową. W ten sposób upraszcza się okablowanie oraz zwiększa bezpieczeństwo instalacji. Zaoferowane czytniki obsługują magistralę lub interfejs Wiegand”.

W treści odwołania wykonawca Mirbud podnosił, że w zaoferowanym przez niego systemie kontroli dostępu firmy UTC kontroler sieciowy działa jako dodatkowy moduł podłączany poprzez interfejs CAN do sterownika sieciowego. Odwołujący wyjaśniał, że w celu spełnienia powyższego wymagania w systemie kontroli dostępu zostanie zastosowana wtyczka softwarowa na poziomie oprogramowania zarządzającego. Powyższe zostało potwierdzone przez Odwołującego w toku rozprawy przez wskazanie, że należy przyjąć, iż zaoferowane przez niego rozwiązanie posiada interfejs, który tłumaczy z protokołu RS485 na CAN.

Biorąc pod uwagę powyższe Izba stwierdziła, że zasadne jest stwierdzenie Zamawiającego o wzajemnej sprzeczności wyjaśnień składanych przez Odwołującego. Z jednej strony Odwołujący wskazuje, że przyjęte przez niego rozwiązanie wykorzystuje interfejs RS485 (str. 5 wyjaśnień) a w innej części tych samych wyjaśnień (tj. na str. 8 wyjaśnień) podaje, że w zaoferowanym systemie kontroli dostępu UTC Fire&Security znajduje się m. in. interfejs CAN. Następnie już w treści złożonego odwołania precyzuje, że w celu uzyskania rozwiązania wymaganego przez Zamawiającego zostanie zastosowana wtyczka softwarowa na poziomie oprogramowania zarządzającego podczas, gdy w dokumentacji wykonawczej brak jest rozwiązania uwzględniającego zastosowanie dodatkowy element, takiego jak wskazywana przez Odwołującego wtyczka softwarowa, która ma doprowadzić do zgodności z rozwiązaniami żądanymi przez Zamawiającego w zakresie interfejsu CAN.

1.4 System kontroli dostępu – czytniki.

W dokumentacji wykonawczej, która stanowiła załącznik do SIWZ w Tomie: II Projekt Architektoniczno-Budowlany Budynek A, w części: VI Branża Teletechniczna, 2.4.8 System kontroli dostępu (str. 70) podano: „Czytniki - W ramach infrastruktury” systemu kontroli dostępu na obiekcie zostaną zainstalowane czytniki oraz karty w standardzie zbliżeniowym MifareD Classic 1k odczytujące numer seryjny karty kontroli dostępu. Czytniki muszą obsługiwać karty dostępu, które Użytkownik posiada na innych obiektach. Czytniki będą produkowane przez tego samego producenta, który produkuje pozostałe elementy systemu kontroli dostępu (sterowniki, kontrolery drzwiowe, oprogramowanie). Gwarantuje to niezawodną pracę całego systemu. Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand, AbaTrack II. Wszystkie elementy elektroniczne znajdujące się wewnątrz obudowy czytnika powinny być zalewane żywicą epoksydową. Dzięki temu czytniki są odporne na niekorzystne warunki atmosferyczne. Czytniki muszą posiadać normę szczelności min. IP65. System KD musi umożliwiać podłączenie szerokiego zakresu czytników kontroli dostępu. System kontroli dostępu musi mieć możliwość komunikacji z czytnikiem za pomocą protokołów szeregowych. System musi obsługiwać czytniki karty z osobnymi modułami Mifare Classic 1k ISO/IEC 14443 Type A”.

Wykonawca Mirbud w piśmie z dnia 23 września 2019 r. podał m. in., że: „Wśród systemowych czytników producenta systemu kontroli dostępu UTC Fire&Security dostępne są zarówno czytniki 125kHz, jaki i 13,6GHz Mifare CSN oraz zapewniające najwyższy dostępny dzisiaj standard ochrony, czyli szyfrowane 13.6GHz Mifire DesFire EV1. W systemie mogą pracować dowolne czytniki obsługujące interfejs Wiegand. Oferta MIRBUD obejmuje wykorzystanie zintegrowanych w systemie czytników ATS1161N pracujących z dwukierunkową magistralą systemową o IP 67 (karta katalogowa czytnika kart zbliżeniowych znajduje się w Załączniku nr 7). W ten sposób upraszcza się okablowanie oraz zwiększa bezpieczeństwo instalacji. Zaoferowane czytniki obsługują magistralę lub interfejs Wiegand”.

W treści złożonego odwołania wykonawca Mirbud przyznał, że wskazany w wyjaśnieniach z dnia 23 września 2019 r. czytnik ATS1161N nie komunikuje się za pomocą któregokolwiek ze wskazanych przez Zamawiającego protokołów transmisyjnych: ani Wiegand, ani AbaTrack II. W ocenie Odwołującego zaoferowanie powyższego czytnika stanowi jednak inną omyłkę polegającą na niezgodności oferty z SIWZ, niepowodującą istotnych zmian w treści oferty, którą Zamawiający mógł i powinien poprawić na podstawie art. 87 ust. 2 pkt 3 Pzp. Poprawa omyłki powinna polegać na zamianie czytnika ATS1161N na inny czytnik produkcji

UTC, czyli czytnik ACI407N wraz z interfejsem czytnika Wieganda ATS1170. Uzasadniając czynność poprawienia omyłki Odwołujący podnosił, że omyłka ta jest konsekwencją wprowadzenia Odwołującego w błąd przez producenta zaoferowanego systemu kontroli dostępu, firmę UTC. Producent, dobierając na etapie składania ofert swoje produkty do wymagań Zamawiającego, wskazał właśnie na czytnik ATS1161N i zapewnił Odwołującego, że czytnik ten spełnia wszystkie wymagania SIWZ.

W toku rozprawy Odwołujący wyjaśnił, że również ten czytnik nie komunikuje się za pomocą jedynie za pomocą jednego z protokołów transmisyjnych Wiegand a nie komunikuje się za pomocą protokołu AbaTrack II.

Wobec tego rozstrzygnięcie wskazanych w odwołaniu zarzutów wymaga przede wszystkim odniesienia się przez Izbę do kwestii wymagań Zamawiającego w zakresie tego, aby zaoferowane czytniki posiadały możliwość komunikacji za pomocą różnych protokołów transmisyjnych, tj. Wiegand, AbaTrack II. W omawianej kwestii Izba podzieliła stanowisko Zamawiającego i Przystępującego, którzy wbrew twierdzeniom Odwołującego, zgodnie twierdzili, że zaoferowane czytniki muszą posiadać możliwość komunikacji za pomocą obu protokołów transmisyjnych, zarówno Wiegand jak i AbaTrack II a nie tylko jednego z nich. Powyższe stwierdzenie Izba oparła na treści zacytowanej powyżej dokumentacji technicznej, w której Zamawiający w odniesieniu do czytników jednoznacznie sprecyzował: „Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand, AbaTrack II”. Dostrzeżenia wymaga, że ww. protokoły transmisyjne są wymienione po dwukropku i zostały rozdzielone jedynie znakiem interpunkcyjnym w postaci przecinka. Na kanwie powyższego Izba uznała, że z powyższego należy wywieść, iż wykonawcę obciąża wymaganie zaoferowania czytników, które powinny posiadać możliwość komunikacji za pomocą obu protokołów transmisyjnych, zarówno Wiegand jak i AbaTrack II. Gdyby chcieć przyjąć za słuszną argumentację Odwołującego, zasadzającą się na tym, że przy doborze czytnika wykonawca może sobie dowolnie wybrać jeden ze wskazanych protokołów to wówczas postanowienie dokumentacji technicznej niewątpliwie zawierało spójniki: „lub” czy też „albo” rozdzielające określone rodzaje protokołów i przykładowo brzmiałoby w następujący sposób: „Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand lub AbaTrack II”. W rozpoznawanej sprawie nie mamy do czynienia z tego rodzaju sytuacją a tym samym Izba uznała argumentację Odwołującego za chybioną. Biorąc pod uwagę powyższe Izba stwierdziła, że brak jest możliwości poprawienia przez Zamawiającego omyłki w zakresie wskazanego czytnika ATS1161N na inny czytnik, tj. ten

wskazywany w treści odwołania przez Odwołującego, bowiem również ten czytnik nie spełnia wymagań Zamawiającego co do możliwości komunikacji za pomocą obu protokołów transmisyjnych, zarówno Wiegand jak i AbaTrack II.

Jednak nawet gdyby chcieć przyjąć za słuszną argumentację Odwołującego, że wymagane było zaoferowanie czynnika, który komunikuje się za pomocą jednego z podanych protokołów transmisyjnych to, w ocenie Izby, brak jest możliwości poprawienia omyłki, polegającej na zastąpieniu czytnika ATS1161N innym czytnikiem, spełniającym wymagania Zamawiającego. Izba stoi na stanowisku, że treść wyjaśnień wykonawcy Mirbud zacytowanych powyżej stanowi treść oferty tego wykonawcy. Zgodnie z ugruntowaną linią orzeczniczą Izby Zamawiający na podstawie art. 87 ust. 2 Pzp jest zobowiązany do poprawy występujących w ofercie wykonawcy omyłek, w tym również innych omyłki polegające na niezgodności oferty ze specyfikacją, z tym zastrzeżeniem, że nie mogą one powodować istotnych zmian w treści oferty.

Na gruncie rozpoznawanej sprawy należy zwrócić uwagę, że informację na temat rodzaju i oznaczenia prawidłowego czytnika Zamawiający uzyskał dopiero w wyniku zapoznania się z treścią odwołania. W tym zakresie Izba za przekonującą i wiarygodną uznała argumentację Zamawiającego, w której podnosił, że na podstawie treści oferty oraz złożonych wyjaśnień Zamawiający nie był w stanie samodzielnie ustalić informacji o tym, czy podanie czytnika ATS1161N jest celowym działaniem czy też omyłką wykonawcy. Jeśli tak, to jaki jest właściwy typ czytnika, który powinien być dobrany przez wykonawcę a nie Zamawiającego, bowiem w takiej sytuacji może się to wiązać z ryzykiem niewłaściwego doboru urządzenia. Zdaniem Izby powyższe wątpliwości potwierdza również stanowisko Odwołującego, który w złożonym odwołaniu wskazał na kolejny czytnik, który został przez Zamawiającego również uznany za niespełniający jego wymagań wskazanych w dokumentacji wykonawczej w zakresie możliwości komunikacji za pomocą obu protokołów transmisyjnych: Wiegand i AbaTrack II.

Izba nie zgadza się również z Odwołującym, że informacje o tym, jaki czytnik powinien zastąpić wskazany przez Odwołującego czytnik ATS1161N Zamawiający mógł pozyskać od Odwołującego zwracając się do wykonawcy o wyjaśnienia na podstawie art. 87 ust. 1 Pzp. W tym miejscu koniecznym jest zwrócenie uwagi na treść wskazanego przepisu z którego wynika, że co prawda w toku badania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Nie mniej jednak niedopuszczalne jest prowadzenie między Zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty, których skutkiem jest dokonywanie zmiany w treści złożonej przez wykonawcę oferty. Izba uznała, że w rozpoznawanym stanie faktycznym poprawienie omyłki prowadziłoby do merytorycznej zmiany

treści oferty Odwołującego w wyniku niedozwolonych negocjacji, które w zasadzie miałyby na celu doprowadzenie oferty Odwołującego do zgodności ze specyfikacją. Poprawienie omyłki w sposób istotny zmieniłoby treść oferty w znaczeniu treści oświadczenia woli wykonawcy zawartego w złożonej ofercie.

Z powyższych względów Izba stanęła na stanowisku, że nawet w sytuacji przyjęcia za zasadne stanowiska Odwołującego, że dopuszczalne było zaoferowanie czytnika posiadającego możliwość komunikacji za pomocą jednego ze wskazanych przez Zamawiającego protokołów transmisyjnych, z czym Izba się nie zgadza i co zostało opisane powyżej, to w rozpoznawanej sprawie nie jest możliwe zastosowanie przez Zamawiającego procedury opisanej w art. art. 87 ust. 2 pkt 3 Pzp w celu zastąpienia wskazanego przez wykonawcę Mirbud czytnika ATS1161N innym czytnikiem, wskazanym w treści odwołania jako spełniającym wymagania Zamawiającego.

1.5 System kontroli dostępu – realizowane funkcje.

W dokumentacji wykonawczej, która stanowiła załącznik do SIWZ w Tomie: II Projekt Architektoniczno-Budowlany Budynek A, w części: VI Branża Teletechniczna, 2.4.8 System kontroli dostępu (str. 71 i nast.) podano: „Realizowane funkcje głównym zadaniem systemu kontroli dostępu jest zarządzanie dostępem do poszczególnych obszarów zlokalizowanych na terenie obiektu. Zaprojektowany system KD ma uniemożliwić wejście do konkretnej strefy KD osobom nieuprawnionym. System KD musi mieć możliwość definiowania harmonogramu terminowego dostępu do stref KD dla poszczególnych użytkowników lub grup użytkowników. Harmonogramy muszą mieć możliwość działania w pętli. Dodatkowo system KD musi umożliwiać definiowanie harmonogramów czasowych definiujących prawa dostępu w konkretnym dniu z dokładnością do jednej minuty.

System musi mieć możliwość generowania raportów na temat ilości osób znajdujących się w poszczególnych strefach, dzięki czemu możliwa jest np. optymalizacja akcji ewakuacyjnej. System KD musi mieć możliwość sprawdzenia gdzie poszczególni użytkownicy znajdują się w czasie rzeczywistym i gdzie znajdowali się w wybranym momencie w przeszłości. Dzięki temu możliwa jest weryfikacja, np. jakie osoby znajdowały się w pomieszczeniu w momencie kradzieży mienia. System KD musi mieć również możliwość obsługi gości poprzez dodanie przez użytkowników do systemu informacji o przyjeździe gościa, którą otrzymuje operator systemu. Dodatkowo musi być możliwość przypisania do danej osoby numeru rejestracyjnego

samochodu. Operator musi mieć możliwość przygotowania dla gościa specjalnej, spersonalizowanej karty z tymczasowymi prawami dostępu do wyznaczonych pomieszczeń, gdzie mają miejsce spotkania.

System KD musi zabezpieczać przed niewłaściwym użyciem karty przez użytkowników oraz sygnalizować sytuacje alarmowe. W tym celu musi realizować poniższe funkcjonalności:

- Funkcję globalnego Anti-Pass Back z podziałem na strefy (wsparcie dla Anti-Pass Back globalnie, punktowo, czasowo, rewersyjnie),
- Funkcję unieważniania kart zbyt długo nieużywanych zabezpieczająca przed użyciem zagubionej karty, np. karta nie użyta na jednym z czytników w ciągu 24 godzin traci swoje prawa dostępowe.
- Funkcję kwarantanny, która zabrania użytkownikom wejście do określonych stref, jeżeli wcześniej znajdowali się w innej, ściśle zdefiniowanej strefie.
- Element ryglujący musi dokonywać zaryglowania przejścia niezwłocznie po zamknięciu drzwi przez osobę wchodzącą do pomieszczenia (element ryglujący nie czeka, aż skończy się czas odryglowania ustawiony w systemie),
- Funkcję wzbudzenia alarmu w momencie gdy drzwi na zbyt długi czas pozostają otwarte.
- Funkcję rozbudowanych alarmów kontroli dostępu, w których alarm jest wzbudzony w momencie gdy karta zostaje uznana jako skradziona, lub użytkownik przyłoży do karte do czytnika do którego nie ma uprawnień.

System musi umożliwiać zmianę stanu przejścia. W systemie muszą być wyróżnione następujące tryby pracy przejścia kontroli dostępu:

- Otwarte - element ryglujący jest nieaktywny;
- Normalny- kontrola dostępu zgodna z harmonogramem i uprawnieniami użytkowników;
- Zablokowany - element ryglujący zaryglowany, czytnik zablokowany i nie odczytuje kart dostępowych.

Wszystkie zdarzenia mające miejsce w systemie są zapisywane w bazie danych systemu.

System umożliwia pełne raportowanie i archiwizację danych. System musi mieć wbudowane predefiniowane raporty, min:

- Raport obecności dla danego użytkownika i dla danego obszaru,
- Raport praw dostępu dla użytkownika i czytnika;
- Raport ścieżki użycia karty na obiekcie;
- Raport stanu sterowników i podłączonych do nich urządzeń;

- Raport kart według grup kart;

Dodatkowo w systemie musi być dostępny generator raportów, który umożliwi generowanie dowolnych raportów według wymogów operatora. Projektowany system kontroli dostępu jest również dostosowany do obsługi przez osoby niepełnosprawne, przez wydłużenie czasu zwolnienia elementu ryglującego w momencie przyłożenia karty przez osobę niepełnosprawną. Dzięki temu osoba niepełnosprawna może bez problemów przemieszczać się po obiekcie”.

Wykonawca Mirbud w wyjaśnieniach złożonych w piśmie z dnia 23 września 2019 r. podał. m. in: „(...)

- 5.1. Zaoferowany system UTC Fire&Security zapewnia harmonogramy terminowego dostępu do stref KD dla poszczególnych użytkowników lub grup użytkowników z dokładnością do HH:mm (do jednej minuty). Harmonogramy mają możliwość działania w pętli.
- 5.2. Zaoferowany system UTC Fire&Security posiada możliwość zdefiniowania stref ewakuacyjnych bezpiecznych, gdzie użytkownicy odbijają swoje karty na czytniku, ułatwiając przeliczenie i raportowanie wszystkich ewakuowanych osób.
- 5.3. Zaoferowany system UTC Fire&Security posiada funkcjonalność zliczania osób wchodzących i wychodzących, celem usprawnienia np. ewakuacji (wiadomo czy wszystkie osoby wyszły z budynku), oraz umożliwia weryfikację miejsca pobytu osób w czasie rzeczywistym i w wybranym momencie w przeszłości (za pomocą zapisu przejść przez drzwi z czytnikami). Warunkiem jest uprzednie odpowiednie zaprogramowanie systemu oraz zaprojektowanie stref, tzw. Anti-passback itp. oraz stosowanych raportów.
- 5.4. Zaoferowany system UTC Fire&Security posiada moduł obsługi recepcji i wydawania kart gości do której oprócz imienia i nazwiska może być przypisany np. numer rejestracyjny samochodu jakim przyjechał. Ww. moduł wymaga awizowania gości, definicji w systemie ścieżek dostępu poprzez wybranie odpowiednich czytników, a wizytę kończy automatycznie odczyt we wskazanym czytniku wyjścia.
- 5.5. Zaoferowany system UTC Fire&Security posiada kilka wersji anti-passback, które działają na pojedyncze drzwi, pary drzwi w jednym kontrolerze lub pary drzwi w systemie. Funkcja może realizować różne warianty funkcjonalności: od logowania niewłaściwego użycia do alarmu o odmowie przejścia włącznie.

- 5.6. W zaoferowanym systemie UTC Fir&Security funkcjonalność, której wymaga Zamawiający, można osiągnąć odpowiednią konfiguracją systemu (zaprogramowanie okresu, po którym następuje unieważnienie karty nieużywanej), bez konieczności dodatkowego oprogramowania, osprzętu, itp.
Można osiągnąć pełną funkcjonalność oczekiwaną przez użytkownika.
- 5.7. W zaoferowanym systemie UTC Fire &Security powyższe funkcje można osiągnąć odpowiednią konfiguracją systemu i kontrolerów, bez konieczności dodatkowego oprogramowania, osprzętu, itp.
Można osiągnąć pełną funkcjonalność oczekiwaną przez użytkownika.
- 5.8. Zaoferowany system UTC Fire&Security zapewnia funkcję wzbudzania alarmu w momencie, gdy drzwi są zbyt długo otwarte. Jest to podstawowa funkcja kontrolerów.
- 5.9. W systemie UTC Fire&Security funkcjonalność można osiągnąć odpowiednią konfiguracją systemu, bez konieczności dodatkowego oprogramowania, osprzętu, itp. Można osiągnąć pełną funkcjonalność oczekiwaną przez użytkownika.
- 5.10. Wzmiankowane funkcje są podstawowymi funkcjami wizualizacji zaoferowanego systemu. System pokazuje wizualnie stany: normalne (zamknięty/otwarty) oraz alarmowe, zmieniając kolory w stanach alarmowych (drzwi zbyt długo otwarte, otwarte siłowo, zablokowane, itd.).
- 5.11. W zaoferowanym systemie UTC Fire&Security wszystkie zdarzenia są zapisywane w bazie danych systemu i korzystając z zapisów zdarzeń można wygenerować podstawowe raporty, które są dostępne od razu (bez dodatkowej konfiguracji). Ponadto istnieje możliwość konfigurowania własnych raportów (można programowo ustawić wszystkie wymagane raporty). System umożliwia pełne raportowanie i archiwizację danych.
- 5.12. Użytkownik zdefiniowany jako potrzebujący/niepełnosprawny będzie miał więcej czasu na pokonanie drzwi. Jest to standardowa funkcja systemu zawarta w kontrolerach. Realizowanie przez zaoferowany system UTC Fire&Security ww. funkcji potwierdza informacje zamieszczone w Załączniku nr 5”.

Odnosząc się do zasadności zgłoszonego zarzutu w kontekście przyczyn odrzucenia oferty Odwołującego powołanych w piśmie z dnia 30 września 2019 r. (str. 3 i 4) stwierdzić należy, że poza przywołaniem odpowiednich treści dokumentacji wykonawczej argumentacja Zamawiającego jest bardzo ogólnikowa i skąpa. W zasadzie ogranicza się jedynie do tego, że:

„Zamawiający uzyskał informację od przedstawiciela producenta systemu kontroli dostępu UTC, że ich rozwiązania nie realizują wszystkich wymaganych przez Zamawiającego funkcjonalności. Zaprojektowany system kontroli dostępu ma zapewniać bezpieczeństwo budynku Komendy Powiatowej Policji w Pile, który wymaga szczególnej ochrony zabezpieczającej przed dostępem osób nieuprawnionych. Zaoferowane przez firmę MIRBUD S.A. rozwiązanie spowoduje niedopuszczalne przez Zamawiającego luki w ochronie obiektu”.

W związku z tym Izba w pełnym zakresie popiera stanowisko Odwołującego w tej sprawie wskazując, że Zamawiający pomimo ciążącego na nim obowiązku nie wskazał w sposób odpowiedni, tj. konkretny i wyczerpujący dlaczego uznał, że rozwiązania zaoferowane przez wykonawcę Mirbud w zakresie realizowanych funkcji nie spełniają jego wymagań. Nie mniej jednak w okolicznościach rozpoznawanej sprawy potwierdzenie się zarzutu naruszenia art. 92 ust. 1 pkt 3 Pzp pozostaje bez istotnego znaczenia dla wyniku postępowania bowiem oferta Odwołującego podlega odrzuceniu z innych przyczyn, wskazanych treści owego uzasadnienia. W pozostałym zakresie Izba uznała zgłoszony zarzut naruszenia art. 92 ust. 1 pkt 3 Pzp za niezasadny.

2. System monitoringu CCTV.

W dokumentacji projektowej w Tomie: II w Projekcie Architektoniczno-Budowlanym Budynek A, część: VI Branża Teletechniczna, 2.4.7 w zakresie systemu CCTV podano: „System musi zapewniać komunikację programową z interkomowym systemem komunikacji gwarantując możliwość realizacji następujących funkcjonalności:

- komunikacja dwukierunkowa pomiędzy serwerami systemu CCTV oraz systemu komunikacji głosowej,
- rejestracja dźwięku z terminali interkomowych zsynchronizowanego z obrazem z niezależnej kamery obsługiwanej przez system CCTV na serwerach systemu CCTV w paśmie nie mniejszym niż 7 kHz oraz metodą kompresji G. 722,
- możliwość odsłuchania przeprowadzonej rozmowy interkomowej z materiału archiwalnego lub w czasie trwania rozmowy z poziomu stacji operatorskiej systemu CCTV,
- przełączanie widoków w trakcie trwania rozmowy prezentujących dzwoniącą osobę,

- kontrola elementów systemu komunikacji głosowej z poziomu widoku systemu CCTV, np. inicjalizowanie połączeń interkomowych, sterowanie przejściami poprzez moduł wejść/wyjść terminali interkomowych”.

Wykonawca Mirbud w piśmie z dnia 23 września 2019 r. podał m. in., że:

1. W zaoferowanym systemie komunikacja dwukierunkowa pomiędzy serwerami systemu CCTV oraz systemu komunikacji głosowej jest zapewniona przez oprogramowanie systemu HIKVISION – iVMS4200, czego dowodzą informacje w Załączniku nr 1 (punkt „Sieć”: „Dwukierunkowa funkcja dźwięku i transmisji” oraz punkt „Ogólne”: „Powiązanie między nadzorem wideo a nadzorem innym niż kontrola wideo (kontrola dostępu, wideodomofon i panel sterowania bezpieczeństwem”).
2. W zaoferowanym systemie rejestracja dźwięku z terminali interkomowych zsynchronizowanego z obrazem z niezależnej kamery obsługiwanej przez system CCTV na serwerach systemu CCTV w paśmie nie mniejszym niż 7 kHz oraz metodą kompresji G.722 jest realizowana poprzez zastosowanie dekodera z serii DS-6900UDI wspierającego metodę kompresji G.722 CCTV w paśmie nie mniejszym niż 7 kHz oraz poprzez zastosowanie rejestratora Hikvision. Na potwierdzenie powyższego przedstawiamy Załącznik nr 2 (Karta katalogowa dla dekoderek z serii DS-6900UDI) oraz Załącznik nr 1, pokazujący jak dekoderek jest wpięty do systemu.
3. Zaoferowany system monitoringu wizyjnego HIKVISION zapewnia możliwość odsłuchania przeprowadzanej rozmowy interkomowej z materiału archiwalnego lub w czasie trwania rozmowy z poziomu stacji operatorskiej systemu CCTV, czego dowodzą informacje w Załączniku nr 1 (punkt „Ogólne”: „Powiązanie między nadzorem wideo a nadzorem innym niż kontrola wideo (kontrola dostępu, wideodomofon i panel sterowania bezpieczeństwem)” oraz punkt „Kontrola dostępu i wideodomofony”: „Zarządzanie wideodomofonem i kontrolą dostępu w jednym module” oraz punkt „Odtwarzanie”: „Natychmiastowe odtwarzanie, normalne odtwarzanie, odtwarzanie wejść alarmowych, odtwarzanie zdarzeń, odtwarzanie ATM, odtwarzanie VCA i odtwarzanie w trybie rybiego oka”).
4. Przełączanie widoków w trakcie trwania rozmowy prezentujących dzwoniącą osobę jest funkcją programową zaoferowanego systemu i jest realizowana przy użyciu oprogramowania iVMS-4200, czego dowodzą informacje w Załączniku nr 1 (punkt „Ogólne”: „Powiązanie między nadzorem wideo a nadzorem innym niż kontrola wideo

(kontrola dostępu, wideodomofon i panel sterowania bezpieczeństwem)” oraz punkt „Kontrola dostępu i wideodomofony”: „Zarządzanie wideodomofonem i kontrolą dostępu w jednym module” oraz punkt „Podgląd na żywo” - cały punkt).

5. W zaoferowanym systemie kontrola elementów systemu komunikacji głosowej z poziomu widoku systemu CCTV, np. inicjalizowanie połączeń interkomowych, sterowanie przejściami poprzez moduł wejść/wyjść terminali interkomowych, jest realizowana za pomocą oprogramowania HIKVISION – iVMS-4200, czego dowodzą informacje w Załączniku nr 1. Topologia systemu przedstawiona została w Załączniku nr 1 w punkcie Typical Applications (Typowe zastosowania). W punkcie tym pokazane zostało jak mogą być ze sobą połączone systemy: CCTV i interkomowy.

W toku rozprawy Odwołujący w zakresie zgłoszonego zarzutu wyjaśniał, że podana przez Zamawiającego liczba urządzeń nie jest tak istotna przy przyjęciu, że na jednym serwerze fizycznym może znajdować się kilka serwerów logicznych, stąd też konieczność zamontowania dodatkowego oprogramowania, które daje możliwość dodatkowych funkcjonalności.

Izba ustaliła, że wykonawca Mirbud w formularzu ofertowym w pkt 7 części A wskazał, że wykona system monitoringu obiektowego CCTV oparty o rozwiązania firmy HIKVISION POLAND Sp. z o.o.

W zakresie rozpoznawanego zarzutu Izba podzieliła stanowisko Zamawiającego oraz Przystępującego, że zaoferowane przez Odwołującego rozwiązania w zakresie system monitoringu obiektowego nie spełnia wymagań opisanych w dokumentacji projektowej. Izba stwierdziła, że w rozpoznawanej sprawie istotnym jest, że rozwiązania znajdujące się w dokumentacji projektowej zostały oparte następujące urządzenia: dwa rodzaje kamer, stacja kliencka, serwery oraz oprogramowania o wymaganych funkcjonalnościach. Natomiast rozwiązanie zaoferowane Odwołującego, aby uzyskać wymagane funkcjonalności musi posiadać jeszcze: dodatkowe oprogramowanie iVMS4200 oraz dekodery z serii DS - 6900UDI oraz rejestrator Hikvision. W kontekście powyższego Izba doszła do przekonania, że zaoferowane przez Odwołującego rozwiązanie nie opiera się o założenia dokumentacji wykonawczej, jak deklarował w treści Formularza ofertowego wykonawca, a jest rozwiązaniem równoważnym względem tego deklarowanego. Na kanwie powyższego Izba uznaje za zasadne stwierdzenie Zamawiającego, że zmiana serwera interkomowego na dekodery, rejestrator i

dodatkowe oprogramowanie to rozwiązanie techniczne niezgodne z dokumentacją projektową o poważnych konsekwencjach technicznych.

Odnosząc się zaś do dowodu przedłożonego przez Odwołującego w postaci oświadczenia firmy HIKVISION POLAND Sp. z o.o. Izba uznała za trafne stanowisko Przystępującego, który w toku rozprawy wskazywał, że treść złożonego dowodu potwierdza jedynie, że autor tego dokumentu jest w posiadaniu systemu o wymaganej przez Zamawiającego funkcjonalności, jednak zupełnie nie wynika z niego, że wykonawca Mirbud w ramach tego postępowania zaoferował takie rozwiązanie.

Na zakończenie prezentowanej argumentacji Izba odniosła się do stanowiska Odwołującego odnoszącego się do dowodów przedkładanych przez Zamawiającego wraz z odpowiedzią na odwołanie oraz w toku rozprawy. Wykonawca Mirbud stwierdził, że składanie dowodów w postaci opinii projektanta i powołanej powyżej korespondencji e-mail - jeśli Zamawiający nie przedłożył, czy też nie powołał ich uprzednio w Informacji o odrzuceniu ofert - to na etapie rozprawy przed Izbą składanie takich dowodów jest spóźnione i niedopuszczalne. Izba zwraca uwagę, że zgodnie z art. 190 ust. 1 Pzp strony i uczestnicy postępowania odwoławczego są obowiązani wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Dowody na poparcie swoich twierdzeń lub odparcie twierdzeń strony przeciwnej strony i uczestnicy postępowania odwoławczego mogą przedstawiać aż do zamknięcia rozprawy. Treść powołanego powyżej przepisu w kontekście stwierdzenia Odwołującego nie wymaga szerszego komentarza a jedynie wskazania, że do zgodnie z jego dyspozycją aż do momentu zamknięcia rozprawy strony są uprawnione do składania dowodów, które uznają za właściwe do wykazania określonych faktów. Tym samym brak jest podstaw do uznania, że powyższe dowody zostały złożone zbyt późno czy też złożenie ich na rozprawie jest niedopuszczalne.

Biorąc pod uwagę powyższe rozważania w rozpoznawanej sprawie Izba stanęła na stanowisku, że treść oferty Odwołującego we wskazywanym zakresie nie odpowiada treści SIWZ a tym samym oferta powinna zostać odrzucona na podstawie art. 89 ust. 1 pkt 2 Pzp. Tym samym Izba uznała, że nie potwierdziły się zarzuty naruszenia przez Zamawiającego art. 7 ust. 1 w zw. z art. 89 ust. 1 pkt 2 Pzp, art. 7 ust. 1 w zw. z art. 87 ust. 2 pkt 3 Pzp. Izba nie dopatrzyła się również naruszenia przez Zamawiającego art. 7 ust. 1 w zw. z art. 87 ust. 1 Pzp. Natomiast zarzut naruszenia art. 92 ust. 1 pkt 3 Pzp potwierdził się jedynie w ograniczonym zakresie, co skutkowało przyjęciem przez Izbę, że pozostaje on bez istotnego wpływu na wynik

rozpoznawanego postępowania, co skutkuje brak możliwości uwzględnienia odwołania na podstawie art. 192 ust. 2 Pzp. O tym przesądza potwierdzenie przez Izbę prawidłowość czynności Zamawiającego, podlegającej na uznaniu, że oferta Odwołującego podlega odrzuceniu na podstawie art. 89 ust. 1 pkt 2 Pzp. W konsekwencji brak jest możliwości uwzględnienia odwołania na podstawie art. 192 ust. 2 Pzp.

Uwzględniając powyższe na podstawie art. 192 ust. 1 i 2 Pzp orzeczono jak w sentencji.

O kosztach postępowania orzeczono na podstawie art. 192 ust. 9 i 10 Pzp stosownie do wyniku sprawy oraz zgodnie z § 1 ust. 1 pkt 2, § 3 pkt 1 i 2 lit. b), § 5 ust. 3 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 15 marca 2010 roku w sprawie wysokości i sposobu pobierania wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania (Dz. U. Nr 41, poz. 238). Izba uwzględniła koszty pełnomocnika Zamawiającego w kwocie 3.600,00 zł w oparciu o przedłożoną na rozprawie fakturę VAT.

.....